NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A MANAGEMENT PERSPECTIVE OF THE DEPARTMENT OF DEFENSE (DOD) INTERNET PROTOCOL VERSION 6 (IPV6) TRANSITION PLAN, WHERE IT IS TODAY, AND WHERE IT NEEDS TO BE BY THE YEAR 2008

by

Peter W. Hart

September 2006

Thesis Advisor:	Geoffrey Xie
Co-Advisor:	John Gibson
Second Reader:	Dan Boger

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2006	**3. REPORT TYPE AND DATES COVERED** Master’s Thesis

4. TITLE AND SUBTITLE: A Management Perspective of the Department of Defense (DoD) Internet Protocol Version 6 (IPv6) Transition Plan, Where it is Today, and Where it Needs to be by the Year 2008.

5. FUNDING NUMBERS

6. AUTHOR(S) Hart, Peter W.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

This thesis focused on the management aspects of the DoD IPv6 Transition Plan. It addressed the management required to transition the DoD computer systems from IPv4 to IPv6. The study identified how computer systems will be affected by the transition from IPv4 to IPv6. The advantages, disadvantages, and risks associated with the transition were analyzed to determine potential areas of improvement. The study provided recommendations that can be used before, during and after the transition. This thesis investigated the ramifications of transitioning to IPv6. It compared the Transition Plan to the current state of preparedness by DoD agencies. It determined whether or not IPv6 can be implemented by 2008. When possible, it identified where the DoD will have to concentrate its effort to ensure the transition goes smoothly and on time.

14. SUBJECT TERMS IPv6, Transition, IPv4, Features, Risk, Cost, RFC

15. NUMBER OF PAGES
103

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

THIS PAGE INTENTIONALLY LEFT BLANK

A MANAGEMENT PERSPECTIVE OF THE DEPARTMENT OF DEFENSE (DOD) INTERNET PROTOCOL VERSION 6 (IPV6) TRANSITION PLAN, WHERE IT IS TODAY, AND WHERE IT NEEDS TO BE BY THE YEAR 2008

Peter W. Hart
Major, United States Marine Corps
B.S., Michigan State University, 1990

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2006

Author: Peter W. Hart

Approved by: Geoffrey Xie
Thesis Advisor

John Gibson
Co-Advisor

Dan Boger
Second Reader

Dan Boger
Chairman, Department of Information Sciences Department

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis focused on the management aspects of the DoD IPv6 Transition Plan. It addressed the management required to transition the DoD computer systems from IPv4 to IPv6. The study identified how computer systems will be affected by the transition from IPv4 to IPv6. The advantages, disadvantages, and risks associated with the transition were analyzed to determine potential areas of improvement. The study provided recommendations that can be used before, during and after the transition. This thesis investigated the ramifications of transitioning to IPv6. It compared the Transition Plan to the current state of preparedness by DoD agencies. It determined whether or not IPv6 can be implemented by 2008. When possible, it identified where the DoD will have to concentrate its effort to ensure the transition goes smoothly and on time.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my thesis advisors, Geoffrey Xie and John Gibson, for setting up the IPv6 working group that provided me the motivation and assistance in completing this thesis. I appreciate the guidance and support they gave me through all stages of this effort.

Many thanks to my great friend William E. Campbell for spending several hours reviewing the drafts of each chapter of this thesis. His insight and assistance helped make sure my thesis was sound.

I would like to thank my parents for the love, support, and understanding that made me who I am today. I would also like to thank Daina’s parents, for without her, I would be lost.

Daina, my lovely bride, I would like to thank you for all of the love and support you have given me. Without your patience and understanding, I would never have been able to complete this thesis. I love you, Pete.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The existing Internet Protocol version 4 (IPv4) was developed in the 1970’s and it provides the basis for today’s Internet interoperability. [Office of ASD, 2005] Internet Protocol version 6 (IPv6) will be the new Internet. It is scheduled to replace the existing Internet Protocol version 4. The Internet Engineering Task Force (IETF) defined IPv6 in Request For Comment (RFC) 1883, which was made obsolete by RFC 2460.

The new protocol will facilitate a major improvement of features which includes communications security, mobility, and the enabling of major networks of sensors and smart tracking tags for integrated, enterprise-centric Government operations. [Geesey, 2006]

The article by Harrison [Harrison et al., 2005] identifies the notable improvements in IPv6 that include extended address space (32 bits in IPv4 to 128 bits in IPv6), extended routing capabilities, simpler and more secure mobile applications, improved security via authentication and privacy features, auto configuration, and increased quality of service (QoS) capabilities.

Internet Protocol provides the critical functionality that enables stable, secure communications between computers across various network types, including local area and wide area networks. In order to assure an effective and secure transition to this new protocol, the Office of Management and Budget (OMB) issued guidance to the Chief Information Officers (CIOs) of all federal agencies on what actions should be taken to support this initiative. [OMB, 2005]

A. PURPOSE OF STUDY

The purpose of this research is to determine the ramifications of transitioning to IPv6 in light of the Governmental mandated transition, particularly the transition of DoD. The purpose of this thesis is to provide evidence of benefits, complexity, and risks that organizations may encounter while transitioning to IPv6. It will compare the Transition Plan to the current state of preparedness by a sample of DoD agencies and determine if

IPv6 can be implemented by 2008. When possible, it will identify where the DoD will have to concentrate its effort to ensure the transition goes smoothly and on time.

B. RESEARCH OBJECTIVE

The objective of this research is to establish the effects that the transition from IPv4 to IPv6 is having on the Department of Defense. An analysis of this area will help determine the benefits and concerns of the transition and develop guidelines to improve its effectiveness.

C. RESEARCH QUESTIONS

The primary research question is: What is the value of transitioning to IPv6? The subsidiary questions are as follows:

1. How will the cost of the new protocol be assessed in terms of complexity and performance?

2. Is it best to transition from the periphery or the core?

3. What risks are involved with the transition?

4. Has the DoD declared its requirement for IPv6 products?

5. Have vendors invented new products or will the DoD first have to specify the requirement?

6. What is the DoD policy with regard to opening the core to new technology?

D. SCOPE, LIMITATIONS AND ASSUMPTIONS

The scope of this thesis will encompass an analysis of the DoD IPv6 Transition Plan in order to evaluate the status of the conversion to IPv6. The study will explore various Request for Comments (RFCs) to establish the progress of the plan. A review of the future transition, in conjunction with the information gathered from outside the DoD, will be used to develop an analysis of the plan. This study was prepared while the Enterprise Architecture (EA) was being generated for submission to OMB. [OMB, 2005] This limits the study from drawing any final conclusions on the success or failure of the transition plan. This study is also limited in that there is not a complete inventory of existing Internet Protocol (IP) compliant devices and technologies. This study assumes that the reader has a general knowledge or familiarity with internet protocols.

E. METHODOLOGY

Multiple research methods were used to answer the primary and subsidiary questions. A broad examination of the available literature was conducted. This examination consisted of the Naval Postgraduate library, the Internet, and theses from various graduate programs.

Interviews were conducted by electronic mail, telephone, and in person with various personnel involved with computer programming and the managing of computer systems, inside and outside of the DoD.

This thesis will provide a qualitative report comparing the transition plan to the current and future status of DoD systems.

Existing publications will be utilized to develop a risk analysis and provide risk mitigation for IPv6**.**

Methodologies needed to support the complicated transition to IPv6, including techniques for implementing and managing the lengthy coexistence of both protocols, are to be analyzed.

Some recommendations for the management of the transition to IPv6 will be derived by examining DoD policy on the introduction of new technology.

F. ORGANIZATION OF STUDY

The remainder of the study is organized as follows: Chapter II will provide a comparison of the two technologies. Chapter III will compare the original transition plan to the current state of preparedness and then conclude with an analysis of the proposed plan to implement IPv6. Chapter IV will analyze the implementation of IPv6 in the DoD. Chapter V will provide the conclusions and recommendations, to include a summary of the research questions and the value of the transition.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

A. INTRODUCTION

This chapter provides a broad introduction about the transition of the DoD computer systems from IPv4 to IPv6. A definition of IPv6 will be provided and the main features will be identified, along with some of the related RFCs. Discussions also include IP addressing, interoperability, weaknesses, and strengths associated with the next generation protocol.

Internet Protocol version 4 (IPv4) is the legacy IP that has been used by the DoD since it was specified in RFC 791 in 1981. [Postel, 1981] It is currently implemented on a wide array of computing and networking platforms.

The Transmission Control Protocol/Internet Protocol (TCP/IP) layering model is also known as the Internet Layering Model or the Internet Reference Model. [Comer, 2004] It contains five layers as illustrated in Figure 1. Among other capabilities, IPv4 uses a 32-bit IP address and it allows unique addresses that number almost 4.3 billion. [UNH-IOL IPv4, 2006] The Internet Layering Model defines formatting of traffic for Layer 3 and it uses IPv4 as the principal encapsulation mechanism. The Internet uses IPv4 to connect devices end to end. Routers have the responsibility of forwarding information across heterogeneous networks.

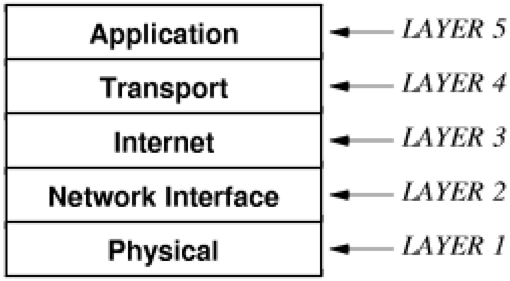


Figure 1. The TCP/IP reference model (From: Comer, 2004)

According to the article by Harrison, the DoD runs the largest IP network in the world. [Harrison et al., 2005] The emerging replacement for the aging IPv4 is IPv6; however, it is not yet widely implemented in North America. Internet Protocol version 6 will coexist with IPv4 and will eventually replace IPv4 in most networks.

The IP resides at Layer 3 and it is a routed protocol. It takes advantage of the routes determined by the underlying routing protocols. The network and host addressing scheme of IP allows for the differentiation and forwarding of traffic between interconnected, disparate local and wide area network links. Layer 3 provides a standard means of transporting data packets to each other across the Internet. Specifically, the formatting of packets sent across an internet is specified by Layer 3 protocols. It also specifies the mechanisms used to forward packets from the source, through one or more routers, to a final destination. [Comer, 2004]

The structure of the US Internet architecture is set up to where it has little problem with the address space under IPv4. Other countries of the world have a lesser allocation of the IP address space [Charny, 2003], so the rest of the world will be moving to IPv6 as a means of mitigating their address space limitations. Security holes, among other things, will exist if the US does not transition to IPv6, leaving itself vulnerable to attack on many levels. Ensuring a smooth transition to IPV6 will help protect US systems from the emerging vulnerabilities related to IPv4.

1. What is IPv6?

Internet Protocol version 6 is a suite of protocols and standards developed by the IETF. This new version was previously called IP-The Next Generation (IPng). [Davies, 2003] Unlike IPv4, IPv6 was to avoid random additions of new features. It was designed to have a minimal impact on upper and lower layer protocols. The IPv6 protocol has a new header format, larger address space, efficient and hierarchical addressing and routing infrastructure, stateless and stateful address configuration, built-in security, better support for QoS, new protocols for neighboring node interaction, and extensibility.

The DoD understands IPv6 is a vital technology that will become critical for its agencies. [AIC, 2005] There is an ever increasing user requirement that needs to be supported, along with the IP-enabled devices that continue to flood the market. In addition to the expanded address space, the new features of IPv6 include improved flexibility, functionality, and information routing; enhanced mobility features; and simplified activation, configuration, and operation of networks and services. The security is expected to improve once IPv6 is fully implemented. [AIC, 2005]

The document that instructs DoD agencies to implement the IPv6 protocol is OMB Memorandum 05-22. It is to be implemented in the DoD network backbone by June 2008. [OMB, 2005] The memorandum directs all agencies to complete two inventories of IP devices and technology (see Appendix A), complete an IPv6 impact analysis (see Appendix B), and develop an IPv6 transition plan. The CIO Council Architecture and Infrastructure Committee was tasked to develop additional guidance and to address the elements identified in Appendix C. [OMB, 2005] An IPv6 transition plan was to be submitted by all agencies. As part of their enterprise architecture (EA) assessment, agencies were to provide a progress report on the inventory and impact analysis in February 2006. [AIC, 2005]

2. IPv6 Feature Overview

The design of IPv6 guaranteed an evolution, rather than a radical change, from IPv4. The key intention in the design of IPv6 was to ease the transition from IPv4. Internet Protocol version 6 was designed to interoperate with IPv4. There are specific mechanisms built-into IPv6 that makes it support the transition and compatibility with IPv4. [IPv6 Features, 2005] According to the IPv6 specification, the following categories contain the primary changes from IPv4 to IPv6:

(a) Large Address Space

The large address space of IPv6 has been designed to allow for multiple levels of subnets and address allocation. A small number of the possible addresses are currently allocated for use by hosts. With IPv6, a much larger number of addresses are available. Address-conservation techniques, such as the deployment of network address translation (NAT), are no longer necessary. [Davies, 2003]

(b) Efficient and Hierarchical Addressing and Routing Infrastructure

The Internet will grow and provide new routing capabilities because IPv6 supports large hierarchical addresses. These capabilities are not built-into IPv4. Anycast addresses, which allow a packet to be processed by any one of a set of designated hosts, can be used for policy route selection. It has scoped multicast addresses which provide improved scalability over IPv4 multicast. The "plug and play" installation is provided by local use address mechanisms. [ANML, 2003]

(c) New Header Format

Some IPv4 header fields have been dropped. Others have been made optional to reduce the necessary amount of packet processing and it limits the bandwidth cost of the IPv6 header. As IPv4 headers and IPv6 headers are not interoperable, a host or router must execute in both IPv4 and IPv6 protocols in order to recognize and process both header formats. The IPv6 addresses are four times as large as IPv4 addresses; however, the new IPv6 header is only twice as large as the IPv4 header. [ANML, 2003]

(d) Improved Support for Extensions and Options

IPv6 can be extended for new features by adding extension headers after the IPv6 header. [Davies, 2003] IPv6 has more efficient forwarding and less stringent limits on the length of options. This is provided by the header options that are encoded in such a way as to allow greater flexibility for introducing new options in the future. As noted earlier, some fields of an IPv4 header have been made optional in IPv6. [ANML, 2003]

(e) Better Support for QoS

Traffic is handled and identified by newly defined IPv6 header fields. A Traffic Class field prioritizes the traffic. A Flow Label field enables packets belonging to a particular traffic flow to be identified by routers and provide special handling for those packets. Since the traffic is identified in the IPv6 header, a packet payload that is encrypted with Internet Protocol Security (IPSec) and Encapsulating Security Payload (ESP) can utilize emerging support for QoS mechanisms. [Davies, 2003]

(f) Built-in Security

Security is built-into IPv6. The ESP header and trailer support options such as authentication, data integrity, and data confidentiality. [ANML, 2003] It provides a solution for network security and interoperability between different IPv6 implementations. [Davies, 2003]

(g) Stateless and Stateful Address Configuration

Host configuration is simplified because IPv6 supports both stateful and stateless address configuration. Stateful address configuration is when an automated address configuration is accomplished with the support of a Dynamic Host Configuration Protocol (DHCP) server. Stateless address configuration is autonomous address configuration in the absence of a DHCP server. The IPv6 addresses are configured for the link by the host device and are referred to as link-local addresses. The hosts may also incorporate addresses derived from prefixes advertised by local routers to generate a globally unique address. If there is no router, hosts on the same link can automatically configure themselves with link-local addresses and communicate without manual configuration. [Davies, 2003]

(h) New Protocol for Neighboring Node Interaction

A series of Internet Control Message Protocol for IPv6 (ICMPv6) messages that manage the interaction of neighboring nodes (nodes on the same link) is called the Neighbor Discovery protocol. The broadcast-based Address Resolution Protocol (ARP), ICMPv4 Router Discovery, and ICMPv4 Redirect messages are replaced by Neighbor Discovery. It has efficient multicast and unicast Neighbor Discovery messages. [Davies, 2003]

3. What is the DoD's Plan for the IPv6 Transition?

The goal of the DoD is to complete the transition to IPv6 for all DoD networking by fiscal year (FY) 2008. It should be done in an integrated, secure and effective manner.

According to the DoD IPv6 Transition Plan of March 2006, all Global Information Grid (GIG) assets being developed, procured or acquired are to be IPv6 capable. They must also maintain interoperability with IPv4 systems. The DoD hopes to build confidence by transitioning significant portions of the GIG to IPv6. The Defense Information Systems Agency (DISA) is to acquire and manage IPv6 addresses for DoD, which includes the establishment of address and naming conventions. There will be no IPv6 implementations fielded on networks carrying operations traffic within DoD until such time that the security concerns are addressed.

The criteria for measuring the success of this transition are included in the new capabilities, upgrades and legacy milestones. Success will be determined by many things. Among them will be the ability of the DoD to transition within the specified timeframe. The transition must also have a means for adjudicating claims that an asset should not transition in the timeframe prescribed. There needs to be a technical strategy that supports IPv4/IPv6 interoperability. There must be an identification of the transition activities, resources, roles and responsibilities. It is essential to have early implementation pilots, test beds and demonstrations. Finally, the Information Assurance (IA) issues must be resolved for the transition to be complete. [Transition Plan, 2005]

4. Related Transition Efforts in the Commercial World

The European industry is supporting IPv6. They are manufacturing devices, appliances and developing applications. Some telephone companies and Internet Service Providers (ISPs) are already providing services. [Palet, undated]

Many commercial U.S. organizations initially dismissed IPv6 as a “don’t-need-it-now technology.” [Patterson, 2006] Patterson asserted that the June 2003 DoD mandate “instantly became the single most important driver for IPv6 adoption in the United States.” [Patterson, 2006]

The commercial information technology (IT) world is taking hold of IPv6. Internet Protocol version 6 functionality is being implemented and aggressively incorporated by many of the largest IT vendors. IPv6 functionality has been added to some software manufacturers’ operating systems, these include Microsoft and Red Hat Linux. [Patterson, 2006]

To establish guidance and interoperability testing platforms, the North American IPv6 Task Force (NAv6TF) and the IETF are leading collaborative technical efforts with DOD groups, educators and vendors. The Moonv6 project is the most notable effort. This project is taking place across the United States at multiple locations and is the largest permanently deployed multi-partner IPv6 network in the world. [Patterson, 2006]

5. Common Methods Used for Risk Analysis of Technology Upgrades

Risk analysis is a systematic use of available information to determine how often specified events may occur, as well as the magnitude of their consequences. It includes identification of the sources of risk, their consequences, and the likelihood of occurrence. Information is gained when analyzing risks and is helpful when evaluating and treating the risks. Acceptable risks are separated from major risks by using information as input. [Sorby, 2003] Risk analysis must be performed throughout all of the phases of the life of the system. The DoD is using various approaches to mitigating the risk associated with the transition to IPv6, but no one particular technique has been identified. Several risk analysis methods will be presented in the following paragraphs.

The most common risk analysis methods used within system development are Preliminary Hazard Analysis (PHA), Hazard and Operability Analysis (HazOp), Fault Tree Analysis (FTA), and Failure Modes, Effects (and Criticality) Analysis (FMECA). [Sorby, 2003]

Preliminary Hazard Analysis (PHA) is used in the early design stage of a system in order to discover hazards early in the development process. [Sorby, 2003] The aim is to identify safety design criteria and requirements, and the identified hazards may be assessed in order to eliminate, reduce or control them.

Hazard and Operability Analysis (HazOp) is a bottom-up hazard identification technique. The purpose of a HazOp study is to identify potential hazards and operability problems caused by deviations from the intent of the design. [Sorby, 2003]

Fault Tree Analysis (FTA) is primarily a means for analyzing causes of hazards, not for identifying hazards. [Sorby, 2003] An undesired system state is specified and the method works top-down to identify all its possible causes or combinations of causes. Preferably, all possible ways the undesirable event could occur should be identified in the process.

Failure Modes, Effects (and Criticality) Analysis (FMECA) is a bottom-up ranking approach to identifying hazards. The analysis identifies possible failure modes of each component in the system, and determines the causes and consequences of the failure modes. This approach can identify possible countermeasures. [Sorby, 2003]

Risk analysis can be used for two different purposes in the design phase: (1) as a tool to specify requirements or (2) as a tool to control the risk level against acceptance criteria. Safety critical faults may be eliminated or their occurrence minimized in the design phase. The consequences of a fault may be minimized, which may reduce the risk [Sorby, 2003]. Risk analysis can be used to analyze the effect of changes or to analyze causes of problems and accidents in the operation phase of the system.

The DoD is using a common approach to mitigating the risk associated with the transition to IPv6, but not necessarily those previously identified. Organizations within the DoD are identifying sources of risk and the consequences are being studied in laboratory environments to determine the likelihood of occurrence. The organizations include, but are not limited to Joint Interoperability Test Command (JITC), DISA, and the Federal Aviation Administration (FAA). These organizations will never be able to reduce the risk to zero, so they must determine an acceptable level of risk. Risks will continue to be analyzed as the transition evolves.

The Education Department is linking its move to IPv6 to more than 200 IT business cases and using them to explain the impact of the new technology on each investment. [Miller, 2006]

The FAA plans to set up three test beds to see how well data packets travel through its administrative network using IPv6. [Miller, 2006] Mark Powell, the FAA’s chief technical director, said that his office was setting up routers to connect laboratories in Atlantic City, N.J., Oklahoma City, and Washington over an IPv6 network. Powell said that this is the FAA’s “risk reduction activity.” [Miller, 2006] The FAA plans to look at the size of the routing tables, the latency, what happens when IPv6 packets are sent and what happens when they transition to IPv6 from IPv4. This method will help the FAA understand the impact of IPv6 on their wide area networks (WANs) and local area networks (LANs). [Miller, 2006]

The techniques of other organizations that are mitigating risk will be further developed in the next chapter.

6. Addressing

(a) IPv4 Addressing

There are 8 bytes, or 32 bits, in an IPv4 address. Computers see an IP address in binary format. The IPv4 address of 10.0.0.1 would be in the binary format of 0000 1010 0000 0000 0000 0000 0000 0001. It is written in dotted decimal simply for human readability. [Mitchell, undated] Thus, each octet, or byte, of an IP address has a range of values from a minimum of zero to a maximum of 255. The range of IPv4 addresses is from 0.0.0.0 through 255.255.255.255. There are a total of 4,294,967,296 possible IP addresses for IPv4. [Mitchell, undated]

(b) IPv6 Addressing

There are 16 bytes, or 128 bits, in an IPv6 address. This larger size means that IPv6 supports more than 340,282,366,920,938,463,463,374,607,431,768,211,456 possible addresses (greater than 3.4 x 10^{38}). [TechNet, 2005]

Internet Protocol version 6 addresses can be extensions of IPv4 addresses. The four bytes to the right of an IPv6 address may be rewritten in the IPv4 dotted decimal notation. For example, the IPv6 address E3D7:0000:0000:0000:51F4:9BC8:C0A8:6420 may be converted to the mixed IPV4/IPv6 notation of E3D7::51F4:9BC8:192.168.100.32. [Mitchell, undated]

B. TRANSITION FROM IPV4 TO IPV6

Internet Protocol version 4 cannot support the capabilities necessary to meet future combat system requirements. The transition to IPv6 will allow the DoD to be IP centric. It will give the DoD the ability to have greater mobility, ad-hoc networking capabilities for dynamic addressing, and security through the embedded IPSec. [Dixon, undated]

The CIO Council Architecture and Infrastructure Committee (AIC) is tasked with publishing IPv6 implementation guidance. [AIC, 2005] The use of Enterprise Architecture (EA) will be addressed by this guidance, which will provide information on how to plan for the enterprise-wide IPv6 transition. The council will address IPv6 transition planning best practices, networking and infrastructure, addressing, information assurance, pilots, testing and demonstrations, applications, standards, and training. It will also address the IPv6 transition, acquisition and procurement.

The Joint Interoperability Test Command (JITC) Advanced Internet Protocol Technology Lab is providing critical assistance to the DoD's Defense Information Systems Agency (DISA) IPv6 Transition Office as they prepare for the eventual IPv6 migration while maintaining existing IPv4 interoperability. [Harrison et al., 2005] DISA is ensuring that DoD IPv6 fielding is coordinated, does not duplicate efforts within DoD and does not introduce interoperability and information assurance risks. DISA will acquire, manage, allocate, and control the necessary IPv6 address space for the DoD. The JITC, as the sponsor of the DoD Interoperability Communications Exercise (DICE) [1] and a participant in the Moonv6 exercise, [2] provides a venue to access all agencies within DoD, as well as the Combatant Commands, including United States Northern Command in their Homeland Defense role. This setting helps to refine and validate requirements and reinforce interoperability as the steering point through the evolving DoD Information Technology Standards and Profile Registry (DISR) RFC. DISA and the Joint Staff, with participation of DoD components and Services, have developed a transition plan leading to full IPv6 implementation by FY 2008. [Harrison et al., 2005]

1. Interoperability

It is common knowledge among the IPv6 community that current IPv6 hardware and software lack fully interoperable mobility and security implementations. They do not interoperate well in a native IPv6 environment (IPv6 with no IPv4 functionality); however, they interoperate well when they are used with IPv4/IPv6 transition mechanisms.

[1] DICE replicates a geographically dispersed joint task force (JTF) environment for the purpose of joint interoperability certification or assessment testing. It provides a forum for testing emerging DoD technologies, allied communications initiatives, regressive testing with legacy equipment and realistic joint military communications training. DICE is the sole DoD exercise whose primary purpose is to generate joint interoperability certifications. [Retrieved on 5 April 2006 from http://jitc.fhu.disa.mil/dice/]

[2] The Moonv6 project is a global effort led by the North American IPv6 Task Force (NAv6TF) involving the University of New Hampshire - InterOperability Laboratory (UNH-IOL), Internet2, vendors, service providers and regional IPv6 Forum Task Force network pilots worldwide. [Retrieved on 27 March 2006 from http://www.moonv6.org/]

2. The RFCs

Request for Comments (RFC) document the results of iterative refinements in particular areas of interest to computer networking and communications. In particular, they go beyond the local area network and data communications arena and embody the process for creating a standard for the Internet. They are the means for proposing, evolving, and publishing new standards on the Internet. The IETF reviews these proposals. [Glossary, 2006] The IPv6 specification was detailed in RFC 2460. This document specifies the basic IPv6 header and the initially defined IPv6 extension headers and options. It also discusses packet size issues, the semantics of flow labels and priority, and the effects of IPv6 on upper-layer protocols. Several other RFCs define the IPv6 domain, as indicated below.

IPv6 uses the Internet Control Message Protocol (ICMP), as defined for IPv4, with a number of changes. The resulting protocol is called ICMPv6 and is discussed in RFC 2463.

RFC 2529 "specifies the frame format for transmission of IPv6 packets and the method of forming IPv6 link-local addresses over IPv4 domains. It also specifies the content of the Source/Target Link-layer Address option used in the Router Solicitation, Router Advertisement, Neighbor Solicitation, and Neighbor Advertisement and Redirect messages, when those messages are transmitted on an IPv4 multicast network." [Carpenter & Jung, 1999]

RFC 2711 "describes a new IPv6 Hop-by-Hop Option type that alerts transit routers to more closely examine the contents of an IP datagram. This option is useful for situations where a datagram addressed to a particular destination contains information that may require special processing by routers along the path." [Partridge & Jackson, 1999]

Stateless IP/ICMP Translation Algorithm (SIIT), which specifies a transition mechanism algorithm, is described in RFC 2765. [Gilligan et al., 1996] "The algorithm translates between IPv4 and IPv6 packet headers (including ICMP headers) in separate translator 'boxes' in the network without requiring any per-connection state in those ‘boxes’. This new algorithm can be used as part of a solution that allows IPv6 hosts, which do not have permanently assigned IPv4 addresses, to communicate with IPv4-only hosts.” [Nordmark, 2000]

RFC 2874 “defines changes to the Domain Name System (DNS) to support the renumberable and aggregatable IPv6 addressing. The changes include a new resource record type to store an IPv6 address in a manner which expedites network renumbering and updated definitions of existing query types that return Internet addresses as part of additional section processing.” [Crawford & Huitema, 2000]

RFC 2893 “specifies IPv4 compatibility mechanisms that can be implemented by IPv6 hosts and routers.” [Gilligan & Nordmark, 2000]

The IPv6 Tunnel Broker is outlined in RFC 3053. The transitional IPv6 global Internet “uses a lot of tunnels over the existing IPv4 infrastructure. Those tunnels are difficult to configure and maintain in a large scale environment.” The development of the tunnel broker model is to “help early IPv6 adopters to hook up to an existing IPv6 network” and “to get stable, permanent IPv6 addresses and DNS name associations.” [Durand, et al., 2001]

The connection of IPv6 domains via IPv4 clouds was also discussed in RFC 3056. This RFC “specifies an optional interim mechanism for IPv6 sites to communicate with each other over the IPv4 network without explicit tunnel setup, and for them to communicate with native IPv6 domains via relay routers.” [Carpenter & Moore, 2001]

The RFC 3142 describes an IPv6-to-IPv4 transport relay translator (TRT). “It enables IPv6-only hosts to exchange {TCP, UDP} traffic with IPv4-only hosts. A TRT system, located between the IPv6 and IPv4 hosts, translates {TCP, UDP}/IPv6 to {TCP, UDP}/IPv4, or vice versa.” [Hagino & Yamamoto, 2001]

RFC 3146 “describes the frame format for transmission of IPv6 packets, the method of forming IPv6 link-local addresses and statelessly autoconfiguring addresses on IEEE1394 networks.” [Fujisawa and Onoe, 2001]

There are many RFCs that document Internet Standards. Several of the main features of IPv6 are cross referenced with the related RFCs in the Table 1.

RFC	Title	Function
1752	The Recommendation for the IP Next Generation Protocol	IPng
1888	OSI NSAPs and IPv6	Addressing
1924	A Compact Representation of IPv6 Addresses	Addressing
1981	Path MTU Discovery for IP version 6	Neighboring node interaction
2080	RIPng for IPv6 (Routing Information Protocol)	Built-in Security / QoS
2373	IP Version 6 Addressing Architecture	Efficient and Hierarchical Addressing and Routing Infrastructure
2374	An IPv6 Aggregatable Global Unicast Address Format	Efficient and Hierarchical Addressing and Routing Infrastructure
2401	Security Architecture for the Internet Protocol	Built-in Security
2402	IP Authentication Header	New Header Format / Extensibility / Security
2406	IP Encapsulating Security Payload (ESP)	New Header Format / Extensibility / Security
2460	Internet Protocol, Version 6 (IPv6) Specification (obsoletes RFC 1883)	New Header Format / Extensibility / Security
2461	Neighbor Discovery for IP Version 6 (IPv6)	Stateless and stateful address configuration
2462	IPv6 Stateless Address Autoconfiguration	Stateless and stateful address configuration
2463	Internet Control Message Protocol (ICMPv6) for the IPv6 Specification	Neighboring node interaction
2464	Transmission of IPv6 Packets over Ethernet Networks	Stateless address configuration
2472	IP Version 6 over PPP (Point-to-Point Protocol)	Extensibility
2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	New Header Format
2526	Reserved IPv6 Subnet Anycast Addresses	Addressing
2529	Transmission of IPv6 over IPv4 Domains without Explicit Tunnels	Addressing and Routing Infrastructure / Neighboring node
2545	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing	Extensibility / Addressing
2675	IPv6 Jumbograms	New Header Format / Extensibility
2711	IPv6 Router Alert Option	New Header Format / Extensibility
2740	OSPF for IPv6	Efficient and Hierarchical Addressing and Routing Infrastructure
2765	Stateless IP/ICMP Translation Algorithm	Stateless address configuration
2858	Multiprotocol Extensions for BGP-4	Extensibility

RFC	Title	Function
2847	DNS Extensions to Support IPv6 Address Aggregation and Runumbering	Extensibility
2893	Transition Mechanisms for IPv6 Hosts and Routers	Routing Infrastructure
2894	Router Renumbering for IPv6	Addressing and Routing Infrastructure
3041	Privacy Extensions for Stateless Address Autoconfiguration in IPv6	Extensibility / Stateless address configuration
3053	IPv6 Tunnel Broker	Routing Infrastructure
3056	Connection of IPv6 domains via IPv4 Clouds	Efficient and Hierarchical Addressing and Routing Infrastructure
3142	An IPv6-to-IPv4 Transport Relay Translator	Routing Infrastructure
3146	Transmission of IPv6 Packets over IEEE 1394 Networks	Link-local addresses and stateless autoconfiguration
3484	Default Address Selection for IPv6	Efficient and Hierarchical Addressing
3627	Avoiding ping-pong packets on point-to-point links	Routing
3775	Mobility Support in IPv6	New Header Format / Addressing / Security
4007	IPv6 Scoped Address Architecture	Neighboring node interaction
4191	Default Router Preferences and More-Specific Routes	Extensibility / Routing Infrastructure
4214	Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)	Efficient and Hierarchical Addressing and Routing Infrastructure
4291	Internet Protocol Version 6 (IPv6) Addressing Architecture	Addressing

Table 1. IPv6 Features Cross Referenced with the Related RFCs

C. COST

There is no way to tell the future costs related to the transition, but there are a few estimates that have been published. Many organizations are unaware of the capabilities of IPv6. Patterson says that the Government should view IPv6 as something they “ought to do” rather than something they have to do. [Patterson, 2006]

RTI International has estimated the Government specific cost for the transition at about five billion dollars over 25 years. [Gallaher, 2006] They indicate that the most costly single year will be somewhere at the midpoint of the transition, at a cost of about $600 million. [Jackson, April 2006] The primary cost drivers will be training and manpower for testing and operations, rather than equipment.

Another estimate was provided by Patterson and he estimated that it will cost organizations, to include Government specific costs, approximately $1 billion a year for the next 25 years to transition from IPv4 to IPv6. [Patterson, 2006] He said that the new protocol could generate $10 billion in cost savings and additional services value every year. [Patterson, 2006] According to Patterson, for every dollar invested in IPv6, an organization could expect a $10 return in cost savings. Only about eight cents per dollar is projected to be used for the actual infrastructure upgrade. The remaining 92 cents will be used by taking advantage of IPv6. The demonstrated cost savings are in four main areas: improved security, increased efficiency, enhancements to existing applications and creation of new Internet-driven applications. This data comes from an economic analysis done for the Commerce Department by scientific researcher RTI International of Research Triangle Park, North Carolina.

D. THINGS WE NEED TO KNOW

It is important to study the performance of IPv6 equipment. Chapter III will discuss risks associated with recovery times for failures, the speed of routing, memory requirements, and QoS issues. The speed of routing will need to be analyzed for its affect on the DoD. Address routing protocols, end to end paths, forwarding, and lookup table implementations are just a few of the risks that need to be examined.

E. STANDARDS

New protocols are still works in progress. The IETF has completed more than 100 standards defining the IPv6 protocols. The Tech Watch Report indicates that there are six active IETF working groups still producing new IPv6 standards. (Tech Watch Report, 2006) The legacy technologies will be around for a while and should not be expected to disappear over night. The National Institute of Standards and Technology (NIST) is expecting a coexistence for the next 10 to 20 years. The risks with standards are that they may not be consistent. It is possible that a standard has wriggle room. Meeting the standard may be possible without meeting the spirit of the standard. For example, devices implementing the standard may conform to those standards, yet may not be interoperable.

F. CONCLUSION

Chapter II provided information about IPv4 and introduced IPv6. It identified some of the issues indicating how the world has outgrown IPv4. Internet Protocol version 6 promises great things for the future; however, only the future will reveal its true potential. The crucial issue for the DoD is how to transition from IPv4 to IPv6. Chapter III will discuss the original transition plan and identify the current state of preparedness. The risks related to the transition will be reviewed to determine whether or not the DoD should transition to IPv6 by June 2008. The remainder of the chapter will be dedicated to the analysis of the implementation plan.

III. IPV6 TRANSITION PLAN

A. INTRODUCTION

This chapter presents the plans, preparedness, and implementation efforts related to transitioning DoD systems from IPv4 to IPv6. It will outline how the original plan evolved and describe why the DoD needed to be the lead agent for change in the United States (U.S.). The primary objective is to understand how prepared the DoD is to make the transition by June 2008. The objective will allow this chapter to conclude with an analysis of the ongoing IPv6 implementation efforts.

B. ORIGINAL TRANSITION PLAN

The DoD Transition Plan describes the overall strategy for the DoD's migration from IPv4 to IPv6. [Office of ASD, 2005] It identifies roles and responsibilities and establishes the foundation for more in-depth efforts.

The efforts intend on accomplishing the transition through a number of elements that protect interoperability, performance and security. Among other efforts, the IPv6 capability must be backwards compatible with IPv4. [Office of ASD, 2005] The IPv6 capability is also required for all procurements and purchases of IT or IT development activities. Another related effort was tasked to the Component Acquisition Executives (CAEs) and CIOs. They are responsible for ensuring the implementation of the procurement policy. There is an effort outlined in the plan for the DoD to reach out to vendors that will participate in forums such as Armed Forces Communication and Electronics Association (AFCEA), Consumer Electronics Association (CEA) and North American IPv6Task Force (NAv6TF). [Office of ASD, 2005] Other details regarding the levels of effort can be further reviewed in the Office of Assistance Secretary of Defense (ASD) Transition Plan of March 2005.

The Office of ASD Transition Plan contains guidance for obtaining IPv6 capable products and the waiver process when products or assets cannot meet transition objectives. It includes guidance for early IPv6 pilot implementations, responsibilities and considerations for transitioning networks, applications, and infrastructure. It establishes the criteria for demonstrating transition readiness and a strategy for leveraging ongoing commercial IPv6 work.

The Transition Plan instructs that the DoD develop recommended network and IA designs, which includes the addition of transition mechanisms and overall implementation schedules. Components were tasked to develop and maintain detailed transition plans for their systems. DISA was tasked to lead the maintenance of the overall plan.

The DoD will implement the transition to IPv6 in phases and the phases will overlap. A milestone in the testing of IPv6 under the Moonv6 project happened in December 2005. It focused on the access layer and IPv4 equivalency. The December event gathered a large number of DHCPv6 implementations at a single location. It included an international Voice over Internet Protocol (VoIP) call made over commercially available software from North America through the use of an IPv6 to IPv4 tunnel. Other areas of testing successfully demonstrated DHCPv6, DHCPv6 prefix delegation, DNS resolution, Voice-over-IPv6 mixed with data traffic, IPv6 mobility, firewall functionality, and IPSec interoperability.

The DoD IPv6 Capable Exercise (DICE) for Moonv6 was designed to evaluate the implementation of IPv6 within the industry from a product commercial-off-the-shelf (COTS) standpoint. The validation of data analysis was tasked to JITC. They also test and evaluate procedures and create DOD IPv6 Approved Products Lists (APL). Program managers select IPv6 capable products tested by JITC and approved by the DoD.

Moonv6 continues to be an active deployment test bed for service providers and suppliers that wish to test and demonstrate IPv6 capable technology. This is an ongoing platform for global IPv6 education and knowledge. The Moonv6 project helps to build a firm foundation of interoperability for the deployment of the next-generation internet.

Dixon described the phases the first will be test and analysis, followed by phases for initialization, implementation of the core, co-existence of IPv4 and IPv6, and then the final transition to a native IPv6 environment. [Dixon, not dated]

1. Test and Analysis

The Test and Analysis phase started in fiscal year 2004 and included the assessments of transition mechanisms and the COTS dual-stack [3] network software upgrades. [Pollock, 2004] To support IPv6 research and test requirements, Defense Research and Engineering Network (DREN) and Defense Information System Network - Leading Edge Services (DISN-LES) have obtained IPv6 capability.

It was expected that, in the FY 05-06 timeframe, at least one core network would natively support IPv6 traffic. [Pollock, 2004] Testing on the "Moonv6" network was conducted from 24 July 2006 to 28 July 2006 at the University of New Hampshire InterOperability Laboratory (UNH-IOL). [Volpe, 2006] Business Wire stated that the Moonv6 network is the world's largest multi-vendor IPv6 network. The testing resulted in the first successful public demonstration of the Network Time Protocol (NTP) running on a native IPv6-only connection. [Volpe, 2006]

In the FY 07 timeframe, the DoD is supposed to have the availability of High Assurance Internet Protocol Encryptor (HAIPE) IPv6 capable devices which will permit the transition of Global Information Grid-Bandwidth Expansion (GIG-BE) and the DoD's other classified core networks to dual-stack operation. In FY 2008, it was expected that IPv6 will be the native protocol with IPv4 being accommodated through tunneling.

The Test and Analysis phase was outlined in a brief by Captain R. V. Dixon. The DoD had to develop a master plan and a transition strategy. [Dixon, not dated] The DoD was going to need to acquire IPv6 address space so that they could develop an IPv6 addressing plan. They needed to plan for the DNS infrastructure modification and establish a DNS root server. The Defense Information Systems Agency (DISA) was assigned to develop an operational laboratory. The DoD needed an IPv6 test bed to analyze modifications to DOD software, perform requirements analysis and IA assessments. They needed to initiate a DOD cost assessment and develop a DOD IPv6 initiation policy.

[3] "Dual IP stack networks and/or hosts with a capability to handle both IPv6 and IPv4. A dual stack host uses a DNS resolver to determine the appropriate IP protocol to use for the intended recipient. In a dual stack network, the routers can forward traffic for both IPv4 and IPv6 end nodes with a dual IP stack." (DoD IPv6 Transition Plan, Office of ASD, March 2005)

2. Initialization

The initialization phase will require a complete DNS infrastructure modification. [Dixon, not dated] It will require that the IPv6 test bed be extended, a cost assessment completed, and resources for information developed. This will begin the edge migration to dual-stack. Core networks must begin to translate or tunnel IPv6. Information assurance functionality and the application conversion to dual-stack must begin in the initialization phase. The core migration to dual-stack must be followed by the IPv6 network management capability. This plan allows for the initiation of a dual-stack and IPv6 customer support. For the remainder of this phase, the DoD IPv6 core implementation policy must be developed.

3. Core Implementation

In this phase, the core is to be migrated to dual-stack so that IPv4 and IPv6 functionality can be supported. Once completed, the DoD will introduce IPv6 native capabilities to the edge of the network. They will then introduce IPv6 native applications. The IA functionality will be finalized. The advanced IPv6 functionality will be introduced and the IPv6 network management capability will be finalized. The core implementation will provide full support for dual-stack and IPv6. The next phase will require the development of the DoD IPv6 co-existence policy. [Dixon, not dated]

4. Co-Existence

The core dual-stack, edge dual-stack, and the IPv6 native will need to be finalized. The advanced IPv6 functionality will be implemented. The dual-stack application conversions must be completed and then IPv6 native application development can begin. To conclude the co-existence phase, they will develop the DoD IPv6 native policy as well as the DoD legacy IPv4 policy. [Dixon, not dated] We will have IPv4/IPv6 co-existence for years to come. To be IPv6 native, there can be no communication with IPv4 systems. The only way that IPv4 can communicate with IPv6 is through transition mechanisms or tunneling, which would make the system non-native.

5. IPv6 Native

During the IPv6 native phase, they will finalize the native IPv6 applications and network devices. They must ensure complete IPv6 functionality. The edge network, devices, and core networks must be migrated to native IPv6. If necessary, they must de-integrate IPv4 and then translate or tunnel IPv4 edge devices/networks through the core. [Dixon, not dated]

C. CURRENT STATE OF PREPAREDNESS OF THE ARMED SERVICES

The approach by the DoD is to establish and participate in an IP distributed test network. They must have a realistic implementation and the architecture to support it. They are looking to make interoperability the guiding principle. [Dixon, not dated] The DoD needs to encourage vendor participation to insure interoperability with other IPv6 systems and IPv4 systems using standard applications. The DoD must be able to demonstrate the ability to use various transition mechanisms. They also need to ensure the new features of IPv6 are beneficial to military applications. The different U.S. Armed Services have contributed in the own ways.

1. Army

The U.S. Army identified interoperability issues with the legacy networks and systems, network address translation (IPv4 / IPv6 gateway), and tunneling. [Dixon, not dated] They leveraged autoconfiguration to reduce their net management burden and had potential enhancements to QoS. The Army determined they would have performance issues with dual-stack networks. They conducted mobile IPv6 experiments and participated in the JITC DICE03 experiments and in the evolution of IPv6 policy. They identified a potential early IPv6-enabled adopter with the Warfighter Information Network-Tactical Network Operation Center-Vehicle. They also participated in the DISN IPv6 testbed.

2. Navy-Marine Corps

The Navy’s IPv6 Transition Plan was developed, reviewed and approved through the coordination efforts of the Navy’s IPv6 Transition Project Office (NITPO) Team at the Space and Naval Warfare Systems Command (SPAWARSYSCOM). [Evans, 2005] The SPAWARSYSCOM NITPO established the Navy IPv6 Steering Group (NISG) as a consensus-based team for development, review and endorsement of the Navy IPv6 Technical Transition Strategy document. This was done under the direction of the Department of Navy (DON) Chief Information Office (CIO) and sponsorship of Chief of Naval Operations (CNO) N71. [Evans, 2005]

The Assistant Secretary of Defense (Networks & Information Integration)/DoD Chief Information Officer [ASD (NII)/DoD CIO] designated Defense Research and Engineering Network (DREN) as a DoD IPv6 pilot network. It is an important DoD resource for research and engineering. The DREN provides connectivity between the High Performance Computing Modernization Program's (HPCMP's) physically separated High Performance Computing (HPC) user sites, HPC Centers, and other networks. [4] The DREN pilot supports DoD Research and Development, Test and Evaluation, and modeling and simulation for classified and unclassified uses.

The HPCMP operates DREN for 4,500 users in DoD and related organizations. It provides leading edge HPC Centers for a nation-wide DoD user community with regard to computers, storage, software, scientific visualization, and user support. It enables DoD HPC software use and it funds development projects.

Space and Naval Warfare Systems Command (SPAWAR) in San Diego, California conducted extensive IPv6 testing over the DREN for three years. They had a test bed between five sites running IPv6 exclusively with multiple operating systems (OSs), firmware (FWs), intrusion detection systems (IDSs), DNS, simple mail transfer protocol (SMTP), and file transfer protocol (FTP). They provided extensive findings and feedback to vendors who were missing functionality, had incompatibilities, and security concerns. [Dixon, not dated]

The SPAWAR Systems Center in Charleston, South Carolina has been a principal participant in Defense Information System Network - Leading Edge Services (DISN-LES) as part of the Commander in Chief 2lst Century (CINC 21) Advanced Concept Technology Demonstration. [Dixon, not dated] They are running a dual-stack environment and have conducted extensive compatibility tests with multiple technologies and products. They share test results to provide real-world experience and to influence hardware and software development and designs.

[4] From the DoD HPCMP website retrieved on 19 August 2006 from http://www.hpcmo.hpc.mil/Htdocs/DREN/index.html

3. Air Force

The U.S. Air Force created the Air Force IPv6 Transition Management Office (TMO) within the Air Force Communications Agency to manage the Air Force's migration from IPv4 to IPv6. The agency developed and updated the Air Force IPv6 Transition Management Plan to version 2.0, completed IPv6 Transition Management Guidelines, was in progress of assessing transition costs at the base and Air Force enterprise levels, and was identifying pilot programs and test equipment and locations in preparation for the 2008 transition. [Spaulding, 2005]

The Air Force has also participated in the DISA-led DOD IPv6 transition working group and the DISN IPv6 test bed network. [Dixon, not dated] They promoted the use of the IPv6 capability in future Air Force acquisitions. The Air Force Information Warfare Center (AFIWC) conducted a security analysis in coordination with the National Security Agency (NSA). They hosted inter-Service IPv6 discussions. The Air Force Research Lab (AFRL) participated in the University of Indiana's Abilene IPv6 test network. The MoonV6 project is also of interest to the Air Force.

D. RISK IPV6 BRINGS TO DOD

There are risks associated with the implementation of IPv6. The next generation protocol will touch everything we do. Figure 2. provides a pictorial of how IPv6 will impact the DoD world.

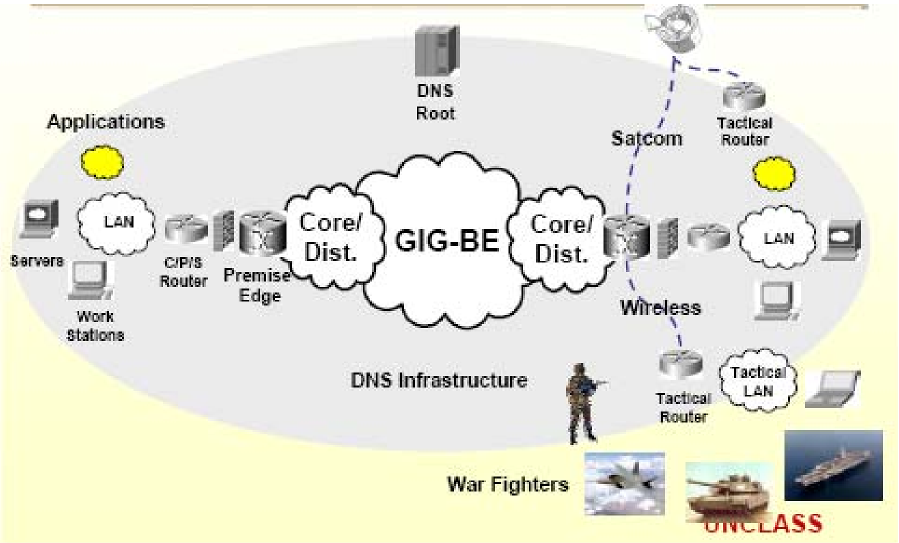


Figure 2. IPv6 will Touch Everything [From: Dixon, not dated]

The DoD intends on ensuring that IPv6 does not introduce interoperability and IA risks. [Dixon, not dated] The temporary restriction of IPv6 on networks carrying operations traffic was designed to reduce the risk associated with interoperability and IA. Figure 3. graphically depicts the projected DoD timeline.

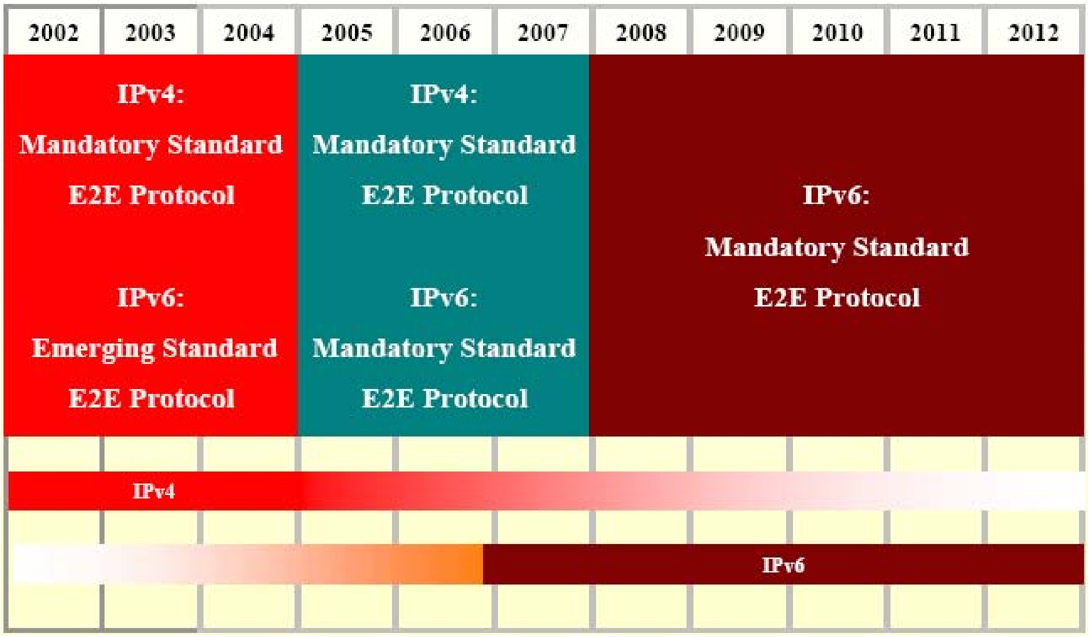


Figure 3. Projected DoD Timeline [From: Dixon, not dated]

1. Risk Areas

Risk areas include software, hardware, technology, cost, schedule, and people. [Osmundson, 2006] There has been little motivation for vendors in the United States to develop software or hardware for IPv6. The technology is out there and is building up around the world, but it is not a priority for U.S. companies. It could be cost prohibitive for many companies, especially small companies. Individual home users will probably not be affected by the transition since ISPs will most likely provide their customers with a dual-stack transition mechanism that will carry IPv4 traffic onto an IPv6 network.

The DoD has been directed to purchase IPv6 compliant hardware. The cost is already being off-set by incorporating this strategy into new purchases. The scheduled transition is for June 2008, it is possible that the schedule will slip prolonging the DoD’s risk associated with IPv4 traffic on an IPv6 network. People tend to be change averse, so they are a risk since they may not want to complete all the tasks necessary to change the way they do business. If it weren't for the DoD, there would be little concern for transitioning to IPv6 in the U.S.

2. Effects

The impact of transitioning to IPv6 will have both positive and negative effects. The DoD will have to focus on the negative impact. The DoD will have to analyze those factors, implement security measures, and be willing to transition to IPv6 with an acceptable level of risk. It is not possible for the transition to be implemented with a risk level of zero, there will be a residual amount of risk the DoD will have to cope with if it is ever want to transition to IPv6.

Experts have identified several effects related to security that IPv6 brings to the network. For example, if Encapsulated Security Payload (ESP) Header is used, the content analysis is impossible for firewalls. [IPv6, 2006] A connection to an untrusted host can be opened up from within a private network when used in tunnel mode, since the IP address will not be visible to the firewall. The effect is that a system becomes vulnerable to fraudulent subnet mask replies as a result of auto-configuration requirements of IPv6, which provides an opportunity for denial of service (DoS) attacks. Strong cryptography is a processor-intensive task and security problems may result from the more complex DNS. It is important to remember that even though IPv6 is designed to provide better security, it does have some negative effects.

3. Deployment Risk

Although the transition is mandated by the DoD, there is a chance that resistance to change may cause some problems. Many producers and users are satisfied with the health and flexibility of IPv4. The large amounts of IPv4 compatible equipment and applications will constrain the transition to IPv6. Users may not be willing to expend capital and labor resources to transition to native IPv6 in a timely manner. If they do not, there could be a security risk that is opened up by an IPv4 user sending traffic through an IPv6 tunnel.

Experts predict that legacy systems will continue to run IPv4 for a long time. [IPv6, 2006] Interoperability of hardware and software will be a major concern for enterprises interconnecting their networks across mixed environments.

4. Economic Risk

Acquiring an IPv6 capability can be accomplished by making the transition a part of the normal technology upgrade or replacement cycle for the DoD. This will allow activities to absorb the cost over a period of time rather than all at once. There should be an extended overlap to minimize deployment and operational interdependencies. It is imperative that IPv6 technology be put in place with operational and security plans, as well as training. Labor will be the largest cost, since IPv6 products will be purchased instead of IPv4 products. The costs will be related to the DoD's existing network infrastructure and operational policy, as well as how the DoD plans to connect to other entities using IPv6. [IPv6, 2006]

5. Security Risk

There will be an increase in security vulnerability at the beginning of the transition, according to experts. [IPv6, 2006] The IPv6 reliance on auto-configuration and other capabilities creates new threats and vulnerabilities. As IPv6 becomes more common among users, the more attackers are likely to turn their attention to breaching IPv6 security. A dual standard mode exposes organizations to increased security risks. Products that are IPv6 capable will undoubtedly be attached to networks regardless of the plans or schedules of organizations. Organizations will need to develop security plans and policies for managing IPv6 traffic. [IPv6, 2006]

6. Implementation Risk

In order to implement IPv6, the DoD must take appropriate steps to ensure it has mitigated risk to an acceptable level. Organizations were directed to identify their infrastructure by an OMB memorandum dated 2005. They also need to identify the scope and objective for the implementation of IPv6. Then the requirements need to be analyzed, followed by the identification of products and activities. Once identifications have been made, this information needs to be passed down to the lower levels. The lower levels can then identify the risks associated with the requirements, products and activities. Then, resources can be allocated to mitigate the risk, followed by a plan that is reviewed and publicized prior to the execution of the plan. Figure 4. presents a method that could be used to plan for the implementation of IPv6. [Osmundson, 2006]

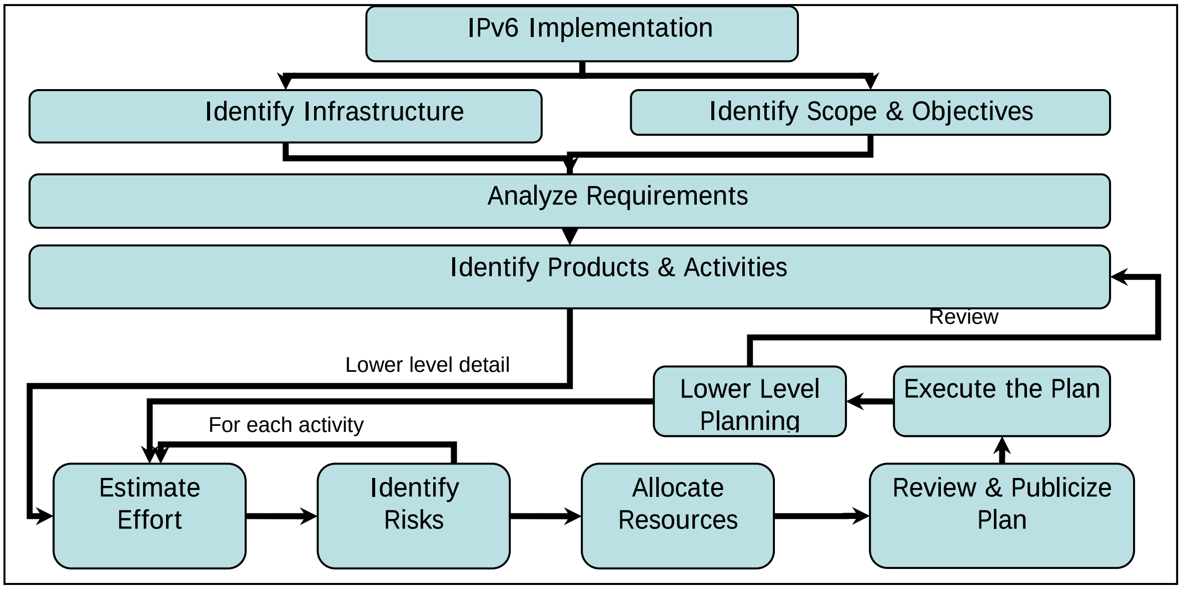


Figure 4. Planning Method [After: Osmundson, 2006]

7. Technological Risk

Internet Protocol version 6 solves the shortage of Internet addresses in Asia. There is a growing opinion that, by adopting IPv6 early, Asia and the European Union will gain a competitive advantage over the United States. [AT&T, 2005] The technological leadership in the Internet may be affected by the resistance to change in the United States.

E. IPV6 STRENGTH

One of the biggest strengths for the Internet throughout the world is that IP addresses will be available for everyone for just about any device imaginable. If the Earth's population was about 6.5 billion, then there will be about 52 octillion (52,351,133,372,452,071,302,057,631,912) IPv6 addresses per person. [Lovering, 2006]

F. IPV6 WEAKNESS

Intrusion detection can be a problem since network administrators may not see the need to worry about IPv6 as long as their needs are met by IPv4. Internet Protocol version 6 is available to anyone with an IPv4 address. Simple commands in internet enabled platforms, that are IPv6 ready, allow users to fully utilize the protocol. Organizations are not likely to be prepared to defend themselves against IPv6-based attacks if they are unprepared to support or recognize IPv6. It is just a matter of time before hackers take advantage of new IPv6 services. Hackers will turn this lack of understanding about IPv6 to their own advantage. [Warfield, 2003]

G. IMPLEMENTATION OF IPV6

The complexity and cost associated with the transition from IPv4 to IPv6 has slowed the adoption of IPv6. As a result, the coexistence of these protocols will be required to support the migration from IPv4 to IPv6 for a long time.

Carrying the IPv6 traffic over the IPv4 network is the key strategy in deploying IPv6 at the edge of a network. The full transition to a native IPv6 backbone will not happen for a while; therefore, this coexistence will permit inaccessible IPv6 domains to communicate with each other.

A white paper from AT&T in 2005 indicated that it is possible to run IPv4 and IPv6 throughout the network. They said it could be done from all edges through the core or it can be translated between IPv4 and IPv6. This allows hosts communicating in IPv4 to communicate with hosts running IPv6.

AT&T says that IPv6-based services can be delivered over a Multi-Protocol Label Switching (MPLS) core network. [5] These techniques allow networks to be upgraded, while IPv6 is incrementally deployed with little disruption of IPv4 services. [AT&T, 2005]

Enterprises in Asia are implementing IPv6 technology. Japan, South Korea and China have federal mandates and incentives for the private sector to adopt IPv6. [AT&T, 2005] China is testing IPv6 networks in cities around the country. Every service

[5] “MPLS is a scheme used to enhance an IP network. Routers on the incoming edge of the MPLS network add an 'MPLS label' to the top of each packet. This label is based on some criteria (i.e. destination IP address) and is then used to steer it through the subsequent routers. The routers on the outgoing edge strip it off before final delivery of the original packet. MPLS can be used for various benefits such as multiple types of traffic coexisting on the same network, ease of traffic management, faster restoration after a failure, and, potentially, higher performance.” Retrieved on 14 July 2006 from http://newsroom.cisco.com/dlls/2004/hd_051904c.html

provider in Japan uses the IPv6 production network. South Korea is working with the European Union to develop applications and services using IPv6. [AT&T, 2005]

Digital mobile devices will use IPv6. The use of IPv6 is mandated in Release 5 of the Universal Mobile Telecommunications System standard (UMTS) from the 3rd Generation Partnership Project (3GPP). The 3GPP develops standards for advanced mobile networks. The UMTS Release 5 mandates IPv6 in all handsets and the 3G [6] Internet Multimedia Subsystem is defined to run only on IPv6.

The high cost of implementing IPv6 in the U.S. has deterred service providers from introducing the new protocol; however, researchers and vendors in the U.S. have exhibited a lot of interest in IPv6. In order to implement IPv6, IP stacks on routers, switches, networking equipment, servers, hosts and other end devices will need to be replaced. [AT&T, 2005]

Internet protocol version 4 is expected to coexist with IPv6. All agencies should be able to run both IPv4 and IPv6 on the network using a dual-stack. They should also be able to encapsulate packets from one IP version to the other. Finally, agencies will need to maintain address translation to ensure IPv4 packets are readable to IPv6 networks and vice versa. [Lost, 2006]

The Defense Information Systems Agency (DISA) is implementing IPv6 over existing DISN core infrastructure's MPLS IPv4 backbone. [Choi, 2006] They are using dual-stack unclassified-provider edge (U-PE) routers. They will use dual-stack access routers as the customers demand service. The provider (P) router functions will remain IPv4. The IPv6 routing architecture / policy will remain the same as the DISN core IPv4.

[6] "The 3G (or 3-G) is short for third-generation technology. It is usually used in the context of cell phones. The services associated with 3G provide the ability to transfer both voice data (a telephone call) and non-voice data (such as downloading information, exchanging email, and instant messaging)." Retrieved on 14 July 2006 from http://en.wikipedia.org/wiki/3G

You can see an illustration of the DISN IPv6 transition in the NIPRNet [7] Diagram shown in Figure 5.

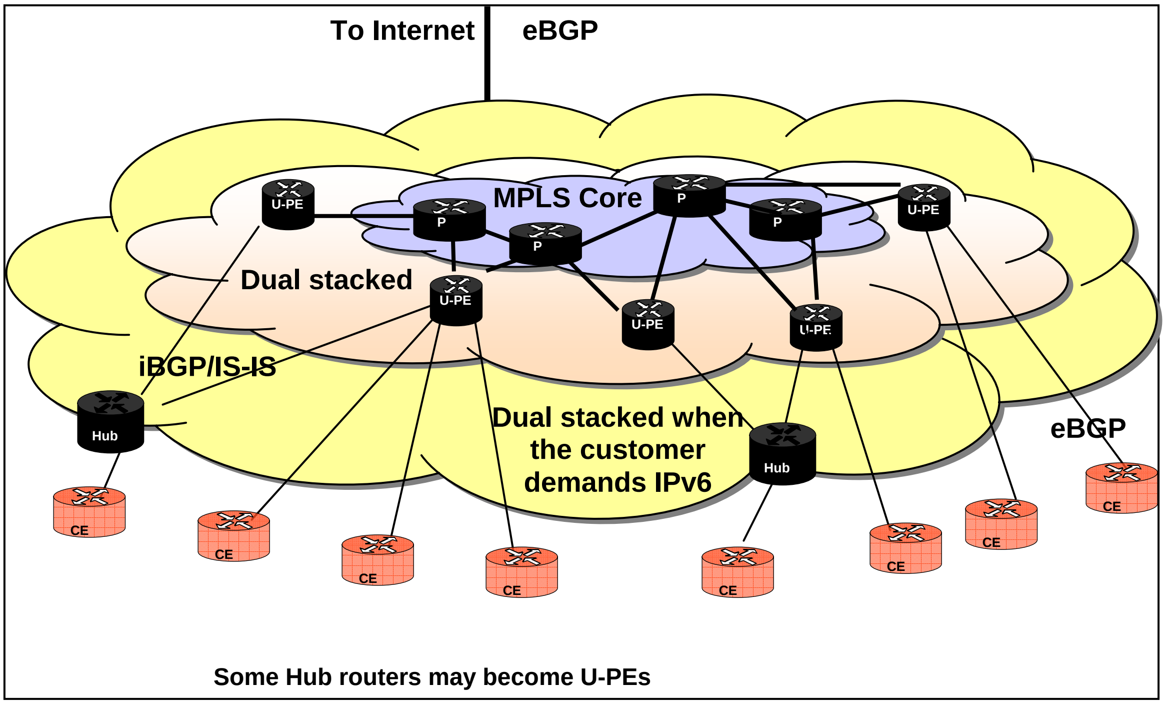


Figure 5. DISN IPv6 Transition: NIPRNet Diagram [From: Choi, 2006]

Choi described the three concentric clouds, seen in Figure 5. as the IPv6 architecture of the NIPRNet. [Choi, 2006] He said that the MPLS core of provider (P) routers is represented by the inner cloud. The P routers will not require IPv6 since they will only transport MPLS packets. The management of P routers will be through IPv4. The unclassified provider edge routers (U-PE) are represented by the middle cloud surrounding the inner cloud. These U-PE routers support both IPv4 and IPv6 on their “outer” interfaces and they are dual-stacked. The aggregation layer of Hub routers is represented by the outer cloud. The aggregation layer will be dual-stacked only if a

[7] “NIPRNET stands for Unclassified but Sensitive Internet Protocol Router Network. It was “formerly called the Non-secure Internet Protocol Router Network.” The NIPRNET is a network of Internet protocol routers owned by the Department of Defense (DOD). Created by the Defense Information Systems Agency (DISA), NIPRNET is used to exchange unclassified but sensitive information between "internal" users as well as providing users access to the Internet. Retrieved on 21 July 02 from http://en.wikipedia.org/wiki/NIPRNET.

customer requires IPv6 service from a service delivery node.[8] The customer edge (CE) routers are outside the three clouds. The NIPRNet will connect to an ISP through U-PE routers. Choi says that the P, U-PE and Hub routers will all be part of the same autonomous system (AS). He lists the protocols between router types as follows [Choi, 2006]:

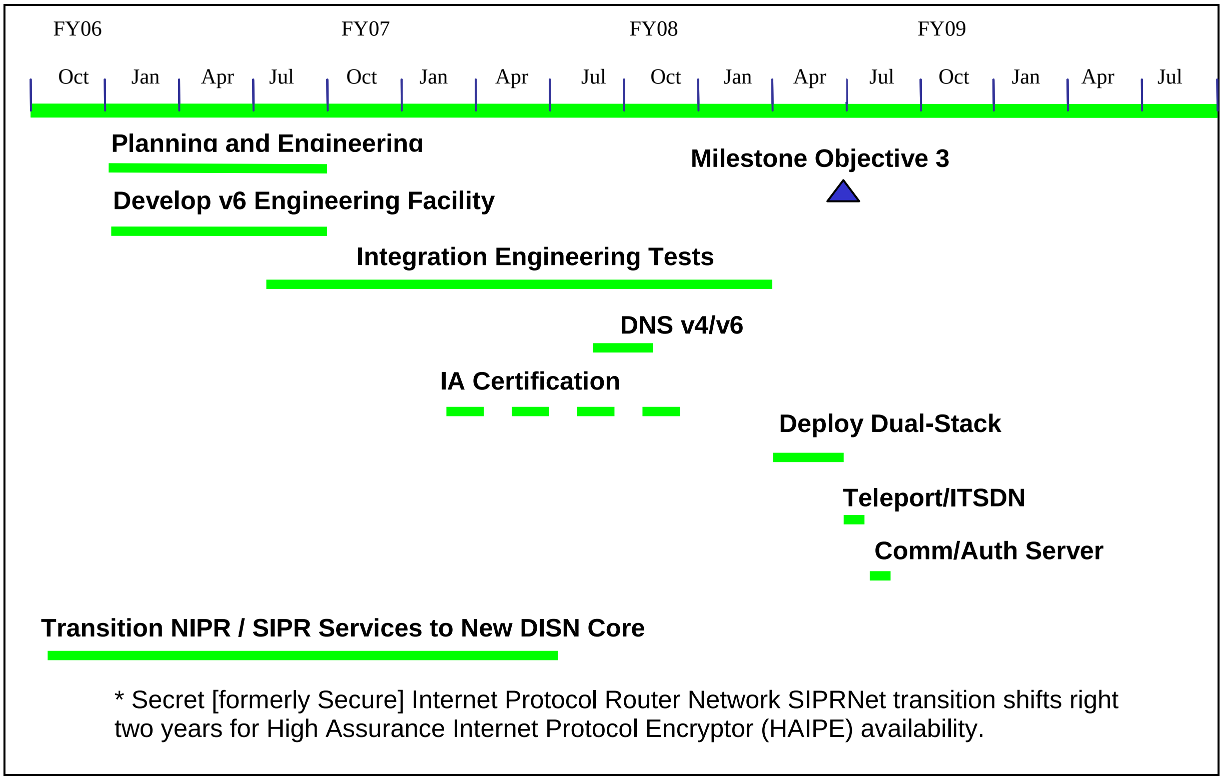
– External Border Gateway Protocol (eBGP) will service CE to Hub, CE to U-PE and ISP to NIPRNet router communications

– Internal BGP (iBGP) and Intermediate System to Intermediate System (IS-IS) will service Hub to U-PE and U-PE to U-PE communications.

Request for Comment 4577 (RFC 4577) indicates that many ISPs offer Virtual Private Network (VPN) services to their customers. It indicates that the DISA technique will work where the CE routers are routing peers of PE routers. The Border Gateway Protocol (BGP) needs to be used to distribute the customer's routes across the provider's IP backbone network. To tunnel customer packets across the provider's backbone, the RFC indicates that MPLS will need to be used. The RFC describes this as a "BGP/MPLS IP VPN". It is presumed in the base specification for BGP/MPLS IP VPNs that the routing protocol on the interface between the PE router and the CE router is BGP.

The plan, as laid out by DISA, shows that the mechanics can work and are backed up by RFC 4577. The final piece of the puzzle is whether or not they can get IPv6 developed, tested, with an IA certification, and deployed by June 2008. Figure 6. shows the NIPRNet schedule for the DISN IPv6 transition.

[8] “A small number of news aggregators have the ability to register to clouds, a web service that notifies the aggregator of updates to a feed, eliminating the need for periodic polling. This approach attempts to produce a more efficient use of bandwidth, though the overhead associated with registering a cloud can mean no net savings. It also introduces issues of scalability and a single point of failure among others.” Retrieved on 21 July 02 from http://en.wikipedia.org/wiki/Aggregator.



* Secret [formerly Secure] Internet Protocol Router Network SIPRNet transition shifts right two years for High Assurance Internet Protocol Encryptor (HAIPE) availability.

Figure 6. NIPRNet Schedule for the DISN IPv6 Transition [From: Choi, 2006]

The aggressive schedule shown in Figure 6. provides a pictorial of the challenges ahead for implementing IPv6 by June 2008. One of the significant issues often overlooked is IA. Without IA, the DoD risks the chance of being infiltrated straight to the core of its communication network.

H. CONCLUSION

Chapter III provided a look at the original DoD transition plan, the state of preparedness, and some of the risks involved with the implementation of IPv6. It identified an approach to implementing IPv6 throughout the DoD. The implementation of IPv6 is complex and will cost a lot of money to make the transition from IPv4. A course of action developed by DISA was presented as a viable option for implementing the transition. However, the implementation of IPv6 has been delayed in the U.S. as a result of the life extension provided to IPv4. A smooth transition and coexistence between IPv4 and IPv6 will require more development. The question still remains to be answered as to whether or not the DoD will actually be able to make the transition from IPv4 to IPv6 by June 2008. Chapter IV provides and analysis of the DoD implementation of IPv6.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ANALYSIS

A. INTRODUCTION

This chapter provides an analysis of the information collected with regard to the implementation of IPv6. A transition strategy will be discussed to outline how at least one segment of the DoD is approaching the transition. This will provide insight into the level of effort being applied and detail why it is vital to the future of DoD operations to transition to IPv6. It will also be used to address an issue that may have been overlooked by the planners of the transition. This chapter will review the position of industry personnel on the importance of a smooth transition to IPv6, but not necessarily as soon as 2008. The viability of current equipment, security, and economics will be discussed as it pertains to the role of the U.S. Government during the transition to IPv6. The first section of the chapter will cover on-going transition efforts and the second section will discuss the identification of potential risks from a systems engineering perspective.

B. ON-GOING TRANSITION EFFORTS

1. Analysis of the Ipv6 Implementation

The DoD IPv6 transition schedule depends upon completion of the transition of NIPRNet and SIPRNet (Secret Internet Protocol Router Network) services to the “new” core. [Choi, 2006] The IPv6 transition should follow a systems engineering approach, as complex problems often have more than one solution and not all of them can be completely solved. The systems engineering approach takes this issue into account.

Systems engineering may be seen as an analysis of the system functional behavior, which requires the system to be partitioned into functional areas. [Osmundson, 2006] The mission needs statement help identify the functional requirements, document the functional baseline, and determine the functional interfaces. Once the top-level needs statement and functional baseline are analyzed, the requirement statements can be developed. Then the requirements must flow down to lower levels so that they can be balanced across the entire system and changes can be negotiated. The approach demands that all requirements be tracked in a traceability matrix. The functional analysis and requirements analysis may then need to be verified.

Choi proposed that the IPv6 transition follow a systems engineering approach and he developed task names, descriptions and schedules. [Choi, 2006] Those tasks are as follows:

> The “Planning and Engineering“ task establishes the general and specific requirements. This task should have covered the January 2006 through September 2006 timeframe. The “Develop v6 Engineering Facility” task augments the existing test bed that supports integration engineering and sustainment activities by including IPv6-related hardware, software and topologies. The task should have covered the January 2006 through September 2006 timeframe. The “Integration Engineering Tests” task should include all activities normally performed prior to the release of a configuration change to the operational network. The task covers the July 2006 through March 2008 timeframe. The “Domain Name System (DNS) v4/v6” task should establish an IPv6 DNS infrastructure on the operational network. The task covers the August 2008 through November 2008 timeframe. The “Information Assurance (IA) Certification” task should include those items required to reach an Authority to Operate (ATO). The task covers calendar year 2007. The “Deploy Dual-Stack” task includes all activities required to deploy IPv6 service on the operational network. The task covers the April 2008 through June 2008 timeframe. The “Teleport/ITSDN” task includes all activities required to deploy both Teleport and Integrated Tactical Strategic Data Network (ITSDN) service on the operational network. The task should take place during July 2008. The “Communication/Authorization Server” task includes all activities required to deploy “CommServer” service on the operational network. The task should take place during August 2008.

The IPv6 transition plan developed an approach; however, it was not to the extent of the systems engineering approach laid out by Osmundson and Choi. The Navy’s transition strategy will now be discussed to determine whether or not the Choi approach was followed.

2. A Transition Strategy

Computer and network infrastructure is impacted greatly by the transition to IPv6. The DoD must field an IPv6 capability and support the requirements of the legacy IPv4 infrastructure. This is a challenge that the DoD faces in its quest for the deployment of IPv6. The DoD plans to transition to the use of IPv6 by having an IPv4/IPv6 dual-stack capability by fiscal year 2008. They began to buy IPv6 capable equipment in 2003.

Future applications and services for both IPv4/IPv6 must be developed in the U.S., especially since they are already being researched by Europe and Asia.

The GIG architecture [9], FORCEnet [10], and Network Centric Warfare (NCW) [11] concepts of operation all indicate that there is an authoritative push to enhance the IP based network capability. The Navy began moving to an IP based network in the 1990s to connect the fleet with the DoD infrastructure ashore. The capabilities ashore were extended to provide the NIPRNet, SIPRNet and JWICS (Joint Worldwide Intelligence Communications System) capabilities in the fleet.

As mentioned earlier, the Navy IPv6 Technical Transition Strategy was developed by the NITPO Team at SPAWARSYSCOM. [Evans, 2005] The Navy's IPv6 Technical Transition Strategy was aligned with the DoD guidance provided to Component Services in the DoD IPv6 Transition Plan of 24 March 2005. This strategy established the Navy's IPv6 program baseline. It identified the critical infrastructure and defined a course of action for the transition of the capabilities. The IPv6 transition is aligned with the FORCEnet transformation along with architecture, standards processes, implementation and planning guidelines. The Navy program managers were provided information on accurate budget submissions, risk reduction and IPv6 capable products.

The Navy's strategy includes a transition approach that accounts for key Navy programs / systems with identified critical infrastructure as early adopters for transition to IPv6. They will use dual-stack networks, addressing plans, deployment product lists, evaluation and certification, intermediate transition mechanisms and then the final transition.

[9] "The GIG vision implies a fundamental shift in information management, communication, and assurance. The GIG will provide authorized users with a seamless, secure, and interconnected information environment, meeting real-time and near real-time needs of both the warfighter and the business user." Retrieved in 5 August 2006 from http://www.nsa.gov/ia/industry/gig.cfm?MenuID=10.3.2.2

[10] "FORCEnet is the operational construct and architectural framework for Naval Warfare in the Information Age which integrates Warriors, sensors, networks, command and control, platforms and weapons into a networked, distributed combat force, scalable across the spectrum of conflict from seabed to space and sea to land." From the CNO's Strategic Study Group - XXI definition from 22 July 02 CNO Briefing.

[11] NCW is "an information superiority-enabled concept of operations that generates increased combat power be networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization." [Alberts, et al., 2000]

The Navy has a high level description of the architecture for the transition to IPv6 within the context of enterprise IT. The architecture includes the implementation of the GIG and FORCEnet, where they focus on technical architectures and standards for the IPv6 transition at the network layer. The IP addressing plans will be developed and implemented in phases.

The Navy created guidelines on the selection of a limited subset of IPv6 transition mechanisms for dual-stack and tunneling to reduce cost, time and risk for migration from IPv4. They have guidance on specific steps to deploy IPv6. A deployment product list was provided to organizations so that they would have a preferred product list and certification from which to work. The core-to-edge deployment of the core critical infrastructure will be conducted in advance of edge applications. The Navy guidance also includes training and operational deployment impacts to the warfighter, test, evaluation and certification.

As the Navy moves closer to implementation, its transition strategy will continue to evolve. The Navy's overall transition approach will occur with an initial phase followed by an intermediate phase and concluding with the final transition. [Evans, 2005] This approach is touted to reduce the cost, risk, technical and scheduling impacts associated with migration of IPv4 to IPv6 over an extended period of time. The strategy is aligned with funding cycles that allow for IPv6 technical refresh to occur over an extended period. The Navy’s goal is to have the Navy's networking infrastructure accommodate both emergent IPv6 and legacy IPv4 traffic.

3. Testing

The United States could isolate itself from the benefits of foreign IPv6 deployments and / or test beds. The DoDs fixed foundation of IPv4 equipment and applications could act as a wall with regard to its transition to IPv6. It is possible, although unlikely; that investors and vendors might not be able to develop new services based on IPv6 or may decide to participate in other market areas. [IPv6, 2006]

The implementation of IPv6 through conformance testing for the standards can and is being completed by the DoD in conjunction with the private sector and other entities. The “Technical and Economic Assessment of IPv6” report indicated that solutions to interoperability problems can be addresses by the DoD by continuing and even expanding its coordination and funding of research. [IPv6, 2006] Protocols, conformance testing methods, and roadmap processes are critical for IPv6 systems developers and implementers. The report also proposed that the U.S. Government coordinate trials and tests of new IPv6 enabled devices. It also indicated that the Government could support IPv6 research into interoperability with existing IPv4 systems.

4. Interoperability

A core capability of IP is the interoperability of hardware and software that interconnects networks across heterogeneous environments. Developers have created dual-stack, tunneling, and translation mechanisms to enable networks to use either or both versions of IP to communicate with each other. These mechanisms are supposed to eliminate dependencies between vendors and networks. This will allow enterprises to decide when to adopt IPv6, if at all. Interoperability will not be seamless in practice. The DoD will have to address any issue related to interoperability problems during the transition from IPv4 to IPv6.

Some experts believe that differences in the implementation of IPv6 could lead to interoperability problems in some areas. [IPv6, 2006] Incompatibility may result since the protocol allows proprietary functions to be incorporated in optional headers. Conformance testing needs to be continued at organizations like JITC. The test beds and activities like Moonv6 need to be continued. If testing is not continued, IPv6 products developed in one company might not be compatible with those developed by another company under the same general standards. In the past, as well as today, there have been times when a standard has been met by a company, but the product may not have actually met the spirit of the standard’s intent. Interoperability should be emphasized during transition to minimize costs and efficiency losses. Since standards include much optional functionality, it is possible to fulfill the requirements of the standard without meeting the spirit of the intent of the standard.

Interoperability can be facilitated by tunneling between IPv6 and IPv4 networks. This increases packet overhead, but it will not create a problem for network routers; however, it will increase the processing time and network overhead costs. [IPv6, 2006]

The DoD can transition to IPv6 at its own pace with interoperability mechanisms. This can lower hardware and software costs and minimize the impact on existing operations.

The DoD must be prepared to protect the wellbeing of U.S. companies by ensuring that IPv6 standards established or implemented by other nations are open, transparent, and not anticompetitive. [IPv6, 2006] Concurrent development activities in Asia, Europe, and the U.S. will likely lead to interoperability issues. Active companies that are involved early on in the process will have the opportunity to influence solutions and gain valuable experience.

In order to minimize adverse effects for users, the transition to IPv6 should move forward in an observant and technology sensitive way. Technical and interoperability issues related to IPv6 can be vetted through the international standards development and coordination bodies.

The DoD has a role to play in the transition from IPv4 to IPv6: it must influence the market to ensure interoperability. It has resources that can provide incentives to the market place. Since the DoD is transitioning to IPv6, industry is on notice that it must make the transition if they want to earn some of the money the DoD will spend over the next several years.

5. The DoD’s Role in the Development of IPv6

The U.S. Government and its agencies will need to coordinate support and participation with industry; however, industry should take the lead in developing the IPv6 standards architecture. The same should be applied to industry groups and academic institutions with regard to conformance testing and the development of interoperability solutions. As a consumer of IPv6 products and services, the DoD has an important role to play. It must continue to evaluate the security and economic factors affecting adoption of the new technology into federal IT systems.

The U.S. Government is a major consumer of IPv6 products and services. [IPv6, 2006] It can affect market evolution by stimulating private sector investment. The timing of IPv6 deployment can be influenced by Government purchases. The DoD will create an initial market of sufficient size to enable suppliers to progress and create product and service performance data for private sector consumers.

Various stakeholders have come to a general consensus that market forces will drive the private sector transition from IPv4 to IPv6. The stakeholders do not believe that there is a significant market hurdle for the adoption of IPv6. They believe that the Federal Government should avoid actions that would significantly interfere with market forces. A comment was made by a representative of MCI that the deployment of IPv6 occurred more slowly than was anticipated, but that there was no evidence of a market failure warranting Government intervention. MCI indicated that the current pace of IPv6 deployment reflects the normal weighing of benefits and costs that is associated with any technology deployment. [IPv6, 2006] Some experts, however, also emphasized that the public sector should foster development and deployment. They were concerned that the U.S. was lagging behind in developing and deploying IPv6 and that U.S. competitiveness and IT leadership could suffer without Government activity.

6. DREN Pilot

The DREN is the “DoD's recognized research and engineering network. It is a robust, high-capacity, low-latency nation-wide network that provides connectivity between and among the High Performance Computing Modernization Program (HPCMP) geographically dispersed High Performance Computing (HPC) user sites, HPC Centers, and other networks. The DREN WAN capability is provided under a commercial contract. The DREN WAN service provider has built DREN as a VPN based on its commercial infrastructure.” [12]

The DoD's largest IPv6 and IPv4 (dual-stack) network can be researched through the DREN Pilot project. The DREN has been in operation since 1992, but it is not Government owned. The DREN is provided as a commercial service by MCI using MPLS on a very high performance Backbone Network System (vBNS+). [Baird, 2004]

[12] The DREN. Retrieved on 19 Aug 2006 from http://www.hpcmo.hpc.mil/Htdocs/DREN.

The latest incarnation of the vBNS was created in 1995 by MCI WorldCom and the NSF (National Science Foundation). The vBNS+ [13] is a very fast fiber-optic network that is one of the test beds for the Internet2 [14] effort to develop new protocols and technologies for businesses, education, Government, and private users. This project is proving the concept of various transition mechanisms from dual-stack, IPv6-to-IPv4 tunneling, IPv4-to-IPv6 tunneling, Dual Stack Transition Mechanism (DSTM), through to Network Address Translation - Protocol Translation (NAT-PT). Figure 7. shows the pyramid structure of the HPCMP.

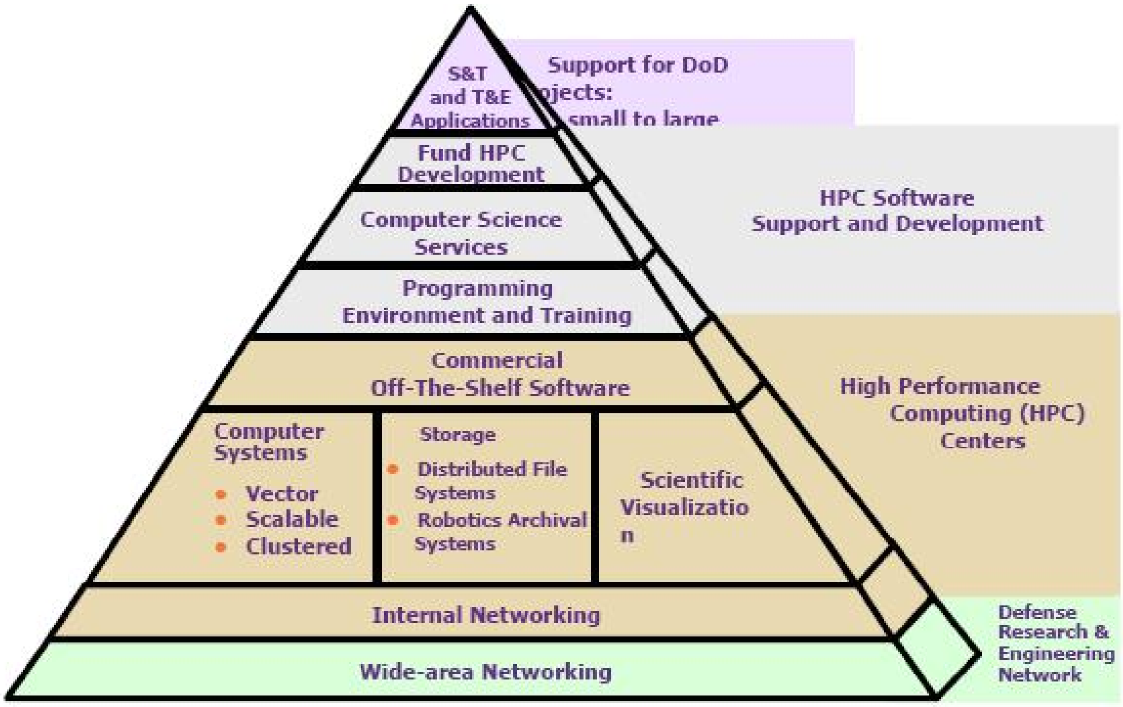

S&T and T&E Applications
Support for DoD ojects: small to large
Fund HPC Development
Computer Science Services
Programming Environment and Training
HPC Software Support and Development
Commercial Off-The-Shelf Software
Computer Systems
Vector
Scalable
Clustered
Storage
Distributed File Systems
Robotics Archival Systems
Scientific Visualizatio n
High Performance Computing (HPC) Centers
Internal Networking
Wide-area Networking
Defense Research & Engineering Network

Figure 7. HPCMP (From: Baird, 2004)

[13] Smart Computing® In Plain English. Retrieved on 19 August 2006 from http://www.smartcomputing.com/editorial/dictionary/detail.asp?guid=&searchtype=&DicID=8005&RefType=Dictionary.

[14] Internet2 is a non-profit consortium which develops and deploys advanced network applications and technologies, mostly for high-speed data transfer. It is led by 207 US universities and partners from the networking and technology industries (such as AT&T, Intel, Sun Microsystems, and Cisco Systems).

7. Easing Concerns

The DoD could provide information on the current status of IPv6 infrastructure and conformance testing requirements. Some networks are not testing and developing IPv6 applications for fear of issues like the interdependence between IPv6 applications and ISP routing services. Access to transition tools and better information could help ease the minds of different organizations. Some experts suggest, however, that markets are pushing IPv6 development and deployment in an appropriate time frame. These experts indicated that the transition mechanisms were designed to avoid the problem of having to "throw a switch." [IPv6, 2006] These experts do not necessarily agree that the appropriate time frame includes the June 2008 transition mandate. Some wonder why the DoD is pushing the transition on this timeline when they expect that the transition will happen over a gradual period of time at an acceptable pace.

A major issue arises over the concern that users may not demand IPv6. Users may not be willing to pay for IPv6-enabled products, since IPv4 works and can also be extended to provide the same functionality as IPv6.

C. RISKS FROM THE SYSTEMS ENGINEERING PERSPECTIVE

1. Asynchronous Transfer Mode (ATM)

The DoD is implementing the transition from IPv4 to IPv6 for systems already running on IP. At the same time, other networks are changing over from ATM to IP. [Buxbaum, 2006] Analysts suggest that the switch from ATM to IP has frequently been overlooked in discussions of the IPv6 transition.

Some analysts say that it will be better if the DoD does not meet its transition schedule. The DoD may want to relax the schedule so that the transition to IPv6 will have a rational, secure and cost-effective result. [Buxbaum, 2006] If the DoD scrambles against this hard 2008 deadline, shortcuts may be taken which might result in irrational decisions, problems with security, and increased costs.

The transition involves upgrading IPv4 to IPv6 for those systems already running on IP. It also involves switching over other networks from ATM to IP. Asynchronous Transfer Mode was designed as a bridge between synchronous channel networking and the packet-based networking characteristic of IP and frame relay communications.

[Buxbaum, 2006] Bit streams of circuit-switched networks and the packet streams of packet-switched networks are mapped by ATM onto a stream of small fixed size cells.

There are tradeoffs to consider when transitioning from ATM to IP. Internet Protocol was developed for maximum flexibility and speed. Unlike ATM, the IP packets can vary in size and more easily support video streams and the convergence of voice, data and video communications. [Buxbaum, 2006] Security and reliability, however, were technological layers added onto IPv4, which slowed down the movement of packets. There is a high level of security and QoS associated with ATM. Unfortunately, ATM lacks the flexibility of IP communications because it works with the small fixed size cells already mentioned. [Buxbaum, 2006] Ralph Havens, president of Marconi Federal, is quoted by Buxbaum as saying,

> In the rush to simplify building applications for IP, people lost sight of the security and quality of service that were always givens in networks of old. You could actually trace circuits in their entirety from one end to another, and you could guarantee a lot of security by preventing physical access to facilities.

The issue here is that ATM had the level of security that Mr. Havens refers to in the previous quote. The virtual circuits were managed end-to-end. Internet protocol uses technology that allows packets to be transmitted using the best route possible. Senders may not know how their packets get from one end to the other. The packets are a security risk, since they are difficult to audit or constrain. A possible reason for overlooking ATM is due to the fact that IPv6 is the technological wave of the future and it is cheaper to operate and maintain than ATM. [Buxbaum, 2006]

Tom Nolle is the president of a technology consulting and analysis company called CIMI. He stated that IP networks will result in a cost savings for the DoD. The refresh and replacement cycle of equipment is involved with the cost of transitioning to IPv6. Once the equipment is replaced, Nolle says that running an IP network instead of “an ATM network of the same capacity” should result in an overall cost savings of “30 percent to 40 percent.” [Buxbaum, 2006] Mr. Nolle made the assumption that operational costs would run about 15 percent to 25 percent in favor of IP if network administrators and operational personnel that brought up ATM networks were trained to equal levels of skill as those working on IP networks.

Transitioning from ATM and IPv4 to IPv6 will be a challenge. The network environments will have increased complexity, higher operating speeds and assured end-to-end security regardless of network, application or location. [Guzelian and Limoges, 2006] Users were allowed to prioritize traffic through the built-in QoS of ATM networks. Asynchronous Transfer Mode supports prioritization better than IPv4; however, IPv6 has QoS mechanisms that allow the deployment of advanced QoS designs. [Guzelian and Limoges, 2006] The complexity of the network will increase as IPv6 improves IP network performance and versatility.

Asynchronous Transfer Mode seems to be overlooked and it may be related to the fact that there is no single policy established in the DoD. The guidance is just that, guidance.

2. DoD Ambiguity

Industry participants and observers don’t see a single focused policy from the DoD. There is still no single integrated policy with all of the pertinent dates of when things should happen, where issues will be resolved, and how the transition will actually be finalized. [Buxbaum, 2006] There are a lot of moving parts, with a lot of agencies doing a lot to support the transition, but they are still missing the focused policy sought by industry.

Mike Guzelian, director for network security products at the information assurance division of General Dynamics C4 Systems, said that it is not possible to meet the deadline since the certified encryptors for IPv6 that they are working on will be released around the same time. He said that the testing evolution will likely take the DoD at least a year. He stated that the DoD will have to update all the switching and routing equipment and that there was not enough manpower to accomplish this all at once. [Buxbaum, 2006]

The senior analyst at Current Analysis, Glen Hunt, says that rushing to implement IPv6 is pointless since the applications are not quite ready for execution. [Buxbaum, 2006] Mr. Hunt is quoted by Buxbaum as saying,

> To decree a transition to IP is one thing, but to actually see technology that supports applications that the military needs is another. Cisco, Juniper, Alcatel and others are all playing strongly in the IP router space and are doing a number of IPv6 trials. But it's not like IPv6 will be ready tomorrow. It's going to be a mixed bag for some time to come.

Industry has been working on a way to encrypt ten gigabit IP streams. [Buxbaum, 2006] Hunt said that there are vendors selling appliances that can convert ten gigabit IP traffic into ATM. The appliance then sends the ATM traffic across the network and reconverts it back to IP on the other end. The ten gigabit encryption development has helped to continue the transition to IP. Hunt also stressed that the market will release more reliable and intelligent IP routers and switches that will smooth the progress of the transition.

Guzelian said that IPv6 beta version software is being put out onto networks. He said that a single machine can carry secret and unclassified traffic as a result of encryption interfaces for personal computers (PCs) and multilevel work stations. [Buxbaum, 2006] A secret connection can be made with authorized personnel and that same single user can maintain a separate connection with coalition partners at the same time.

The DoD may have been the catalyst for the transition to IPv6, but industry will have to accelerate the move to IPv6. Industry will have to commit resources to IPv6 for growth, performance and application benefits. Industry will have to continue working with the DoD to implement IPv6 to develop the Net Centric Warfare concept of operations, to join applications, take advantage of IP television, IP video, IP telephony and service-oriented IP data networking.

3. Intelligence Concerns

The Information Sciences Institute (ISI) at the University of California prepared the Internet Protocol Defense Advanced Research Projects Agency (DARPA) Internet Program Protocol Specification in September 1981 and called it RFC 791. It was prepared for DARPA to specify the DoD Standard IP. It revised the Advanced Research Projects Agency (ARPA) IP addressing, error handling, option codes, and the security, precedence, compartments, and handling restriction features of the IP. The DoD made TCP/IP the standard for all military computer networking in 1982. [Hauben, 1998] Eventually, the computer industry helped popularize the protocol, which lead to increased commercial use.

The physical security at network end points dissolved when IP was opened to commercial use. Nolle indicated that the intelligence community is concerned with the advertisement of false routes to the network. The intelligence community may also be worried that IP encryption will be inadequate for intelligence purposes. Nolle said that he expects significant "pushback" of the transition from users and administrators of intelligence networks. [Buxbaum, 2006] Nolle's assumption that some people in the intelligence community do not accept the level of security offered by IP will be addressed in the flowing paragraphs.

Chen [Chen, et al., 2004] defined IPSec as a tunneling protocol that "not only provides encapsulation/decapsulation but encryption/decryption and hashing." Their article, "Tunnel Minimization and Relay for Managing Virtual Private Networks", said that "an IPSec tunnel often fails to be established due to the management complexity." Their work proposed the concept of "authority to alleviate the management overhead by reducing the number of tunnels." They described the complexity of establishing an IPSec tunnel between two VPN gateways. They indicated that administrators need to negotiate several policies, like the Internet Key Exchange (IKE). They went on to explain that "administrators must specify the packets to be transmitted or received through this tunnel, the negotiation mode (main or aggressive) of IKE phase 1, the required sub-protocol (ESP or AH), the encryption algorithm (DES or 3DES), the hash algorithm (MD5 or SHA1), and the PSK (Pre-Shard Key)." [15] For this reason, tunnels are not frequently established. They favored the use of fewer tunnels to reduce the overhead. Chen, et al., restated that "packets that originally appear in a reduced tunnel are relayed to others,

[15] AH is Authentication Header; DES is Data Encryption Standard; 3DES is a triple strength version of DES.

violating the requisite for private communication through an IPSec tunnel between two VPN gateways." [Chen, et al., 2004] This indicates that IPsec alone may not fill the requirements desired by the intelligence community.

In the article by Buxbaum, Nolle noted that security issues would not have a large role in much of the traffic carried on military networks. He estimated that 60 percent to 70 percent of the traffic is similar to the traffic carried on private sector networks. [Buxbaum, 2006] Nolle indicated that the DISA strategy to transition to IP will impact all military processes. He hypothesized that some specialized networks involving military applications have not transitioned and that the transition, although mandated, might be resisted.

Security concerns are being successfully addressed through the National Security Agency's (NSA's) commercial communications security (COMSEC) endorsement program. The NSA's certification of wireless Internet encryption technology is leading to the possibility of sending Top Secret (TS) e-mails from just about anywhere. A modular IP encryption device will allow users to send classified data and voice messages using unsecured private and public networks. [Hawk, 2005]

SecNet 54™ was built by Harris Corporation under the NSA's COMSEC endorsement program. The device is undergoing NSA's type-1 encryption certification process and an NSA-certification of TS and below is expected in the Fall of 2006. [Hawk, 2006]

The product overview [SecNet 54™, 2006] provided by the Melbourne, Florida-based Harris Corporation, defines the SecNet 54™ device as:

> The generic name for Harris Corporation's new family of Internet Protocol (IP) communications encryption products, designed to keep data, voice, and video communications secure. This product is comprised of a modular architecture with two components: a Cryptographic Module (CMOD) that provides all security-critical functions, and an External Module (XMOD) that handles the transport of encrypted data over specific protocols. Its modular design enables the attachment of a variety of XMODs, allowing secure yet quick and easy utilization of standard communication technologies such as wired 802.3 ethernet, ISDN/PSTN, and wireless 802.11 and 802.16. With its versatility, small size, and up to

> Top Secret wireless and wired communications capabilities, SecNet 54 offers users a cost-effective alternative to traditional, bulky, in-line network encryption devices.

The DoD has made equipment replacement a part of the transition plan to move to IP. They have built-into the plan a course of action to deal with purchasing equipment. As equipment is purchased or becomes obsolete, it is replaced in the normal maintenance cycle with hardware and software that is IPv6 capable.

4. Obstacles

There are a number of obstacles that face the deployment of IPv6. There is a lot of IPv4 compatible equipment and applications that are embedded in today's systems. Many administrators, especially in the U.S., believe that IPv4 is robust enough and flexible enough to meet the needs of the typical producer and user. This comfort zone that administrators have with IPv4 will most likely hold back the rate of migration to IPv6. [IPv6, 2006] It will take capital to fully realize the potential end-to-end communications capabilities of IPv6. Additional capital will need to be expended and labor resources will be required to transition to the new protocol. The total cost of replacing or upgrading all hardware and software to be IPv6 compliant is unknown but could range in the billions of dollars.

Experts predict that legacy systems using IPv4 will exist long after most other Internet users have migrated to IPv6. [IPv6, 2006] Interoperability of hardware and software will be a problem for enterprises that want to interconnect their networks across mixed environments. In an enterprise's decision to adopt IPv6, interoperability will be a major consideration.

Vendors and ISPs are not being pushed by the American public at large to deploy IPv6 products and services. The DoD has pressed the issue by mandating that its agencies purchase IPv6 compliant equipment; however, the demand for IPv6 is still not currently high enough to warrant any kind of urgency from the private sector in the U.S. Potential buyers are uncertain about products and services regarding IPv6 benefits. Users are risk averse with respect to potential innovations. The onus is placed on the organizations who first demonstrate the new technology's potential. These pioneers can be discouraged by a costly and incomplete infrastructure, including standards.

5. Economics

To acquire the IPv6 capability in a short period of time will be more expensive than making the transition as part of an organization's normal upgrade and replacement cycle. [IPv6, 2006] The IPv6 transition mechanisms were designed to allow IPv4 and IPv6 to exist together. Experts believe that ISPs and Internet users should replace IPv4-only hardware and software through their normal product refresh cycles. In order to transition to IPv6, operational plans must be created, security plans developed, and training provided to ensure that the transition occurs effectively. If organizations replace a majority of their equipment during the normal refresh cycle, most of the costs related to the transition will be associated with training, installation, and testing instead of equipment.

The DoD will likely incur greater costs, since it is such a large organization. The size of those costs will depend on the existing network infrastructure and operational policies. [IPv6. 2006] The modification of custom applications will result in additional costs. Additional costs will be generated, since the DoD will have to connect to other organizations using IPv6.

Economics and security go hand in hand. Security is required in today's world, and it is expensive.

6. Security

One of the greatest potential benefits of IPv6 is security. The security is considerably different than what is typically employed in today's networks. Designing and developing new security models will take substantial time and expense. This new and effective security standard should benefit all existing and potential Internet users. Generally, experts agree that implementing IPv6 in the near term will involve an initial time of increased security vulnerability. [IPv6, 2006] New threats posed by a dual standard environment will require additional resources. The IPv6 protocol has new capabilities, such as auto-configuration, but new threats and vulnerabilities will emerge and need to be addressed to avoid abuse.

Attackers will undoubtedly give IPv6 more attention as IPv6 becomes more prevalent. Many security issues will likely arise and will need to be addressed. The DoD is working on security plans and policies for dealing with IPv6 traffic. The DoD will need to continue to devote resources to test and evaluate its capabilities. The impact of transition mechanisms on security architectures will need continuous evaluation. The DoD needs to ensure the security and stability of networks during the transition and establish the best practices for new security policies and management mechanisms.

The U.S. Department of Commerce *Technical and Economic Assessment of IPv6* indicated that more security holes will be found in IPv6 and its related transition mechanisms than in IPv4. [IPv6, 2006] It stated that in the first few years of significant IPv6 use, their will be no better security than what can be realized with IPv4-only networks. The increased use of end-to-end security mechanisms may improve security.

A way to provide security to a network is through the use of firewalls. The use of firewalls at the perimeter will reinforce the use of firewalls at the core of the network. This will help to protect the core and support the transition through an incremental implementation. Most enterprises consist of a limited number of interconnection points where network links are partitioned into external segments, internal private segments, and internal public segments. [16] Security devices are placed at the intersection of each of these segments. They enforce site-wide security policies, provide security services, and monitor traffic for security events. [IPv6, 2006] Virtual private networks may be used to securely connect one trusted network to another, given the implementation includes data encryption, such as that provided by IPSec feature of IPv6. Network Address Translation devices allow the private segments of the enclave to use private addressing. Perimeter based security models provide an advantage in that they focus on site security definition, management, enforcement, and auditing at certain points in the network. These perimeter security points are under the control of enterprise security organizations. These assets are

[16] External segments need network layer access outside the enterprise. Private segments do not require access to hosts in other enterprises or the internet at large; however, some private segments may need access to a limited set of outside services (i.e., E-mail, FTP, netnews, or remote login). Retrieved from RFC 1918 on 18 August 2006.

highly maintained and monitored in enterprise network infrastructures. Audit functions that are centralized allow for easy integration with equipment. [IPv6, 2006]

The security at the perimeter is important. But it is also important to ensure that mechanisms at the core and periphery can interoperate.

D. SUMMARY

Chapter IV provided a look at the issues related to the early stages of transitioning to IPv6 in the United States. It provided an approach to trace the progress of the transition. The Navy's transition was discussed to provide a possible solution for other agencies. It also presented a few issues that may need to be further researched to ensure they are included in the transition. This chapter reviewed the position of industry experts and most believed there was no rush to transition to IPv6.

E. CONCLUSION

The benefits and costs of potential market applications are uncertain. There exists a consensus among experts that the long term adoption of IPv6 is important. The current market driven adoption of IPv6 by the private sector is moving at a practical pace. An efficient migration will occur at an acceptable cost as a result of transition mechanisms; however, other countries are adopting IPv6. This could change the situation and the complexity of the infrastructure necessary to effect the transition from IPv4 to IPv6. It is likely that the transition will require additional support. Technology and economic policy issues need to be examined regularly in order to determine what support may be needed for the growing IPv6 activities by industry, the federal, state, and local governments.

The DoD should consider moving forward with the transition but not fixate on the 2008 deadline. The DoD can concentrate on a smooth transition as systems are replaced through the normal technical refresh cycle.

V. CONCLUSIONS AND RECOMMENDATIONS

A. INTRODUCTION

This thesis examined the DoD transition plan from IPv4 to IPv6. Based on the DoD's Transition Plan and public information about IPv4 and IPv6, the movement from IPv4 to IPv6 will be influenced by the Government and private industry in the United States, as well as the international community. This is necessary since the United States will take a "back seat" in the global IT arena should it transition at its own pace rather than keeping up with the transition taking place in Europe and Asia. In the United States, the DoD has shown a significant amount of initiative in the transition to IPV6; however, globally, the United States is behind Europe and even further behind Asia. Chapter 3 described how every service provider in Japan uses the IPv6 production network and South Korea is working with Europe to develop applications and services for IPv6. The same cannot be said for the U.S.

Internet Protocol version 4 is a protocol that has been in use for over 20 years and it allows computers to communicate across diverse infrastructures. The Internet, and most other data networks, uses IPv4. In the 1980's, the number one bandwidth usage was related to electronic mail. In the 1990's, the number one usage moved over to the emerging world-wide-web access. At the forefront of the development of IPv6 was the proliferation of user devices and successful high utility applications. For example, IPv4 address space became too limited to keep up with the explosive growth so efforts were initiated to mitigate that constraint. Those efforts resulted in the establishment of IPv6. Today, the number one usage is peer-to-peer (P2P) file sharing. Tomorrow, the DoD will use many mobile P2P Services. [Baird, 2004] The transition to IPv6 is necessary to keep up with the technological world.

Internet protocols provide the set of rules that define how computers can communicate with each other across heterogeneous network infrastructures. They use individually routed packets rather than dedicated, switched circuits. Most online systems now use IPv4 as the network layer protocol which is responsible for forwarding these packets between routers and other network devices, but the move toward IPv6 is well under way.

Request for Comment 2460 describes how IPv6 is a new version of the IP and that it was designed as the successor to IPv4. The changes from IPv4 to IPv6 are listed in RFC 2460 and fall into the primary following categories:

1. Expanded Addressing Capabilities:

Request for Comment 2460 identifies that IPv6 will have a four-fold increase in network address space that will provide for greater flexibility in network hierarchical design as well as implementation of autonomous host configuration. Internet Protocol version 6 has the ability and flexibility to meet the growth requirements of multicast routing by adding a "scope" field to multicast addresses. The new type of address is called an "anycast address" and it is used to send a packet to any one of a group of nodes.

2. Header Format Simplification:

According to RFC 2460, IPv6 simplifies the header fields. It reduced the common-case processing cost of packet handling and limited the bandwidth cost of the IPv6 header.

3. Improved Support for Extensions and Options:

More efficient forwarding results from the way IP header options are encoded. The encoding changes also allow for less rigorous boundaries on the length of options as wells as a greater flexibility for initiating new alternatives in the future.

4. Flow Labeling Capability:

The labeling of packets belonging to particular traffic "flows" is a new capability identified by RFC 2460. The sender can request special handling for services such as non-default QoS or "real-time" service.

5. Authentication and Privacy Capabilities:

The final primary category of changes brought by IPv6 is that authentication, data integrity, and data confidentiality are supported by extensions specified for IPv6.

The need to consistently assess the transition from IPv4 to IPv6 and its impact on the DoD's computer architecture will continue well into the future. The challenge is to allow organizations the autonomy to go after the best available assets for the DoD without strictly defining how to accomplish the task. The DoD must transition to IPv6, but it must also measure the cost incurred to ensure the transition is smooth but not strangled by an arbitrary deadline currently set for 2008. The goal is to have agency backbones IPv6 capable by 2008, so that they are ready to accommodate IPv6 traffic; however, they will not necessarily have to pass IPv6 packets.

B. ANSWERS TO RESEARCH QUESTION

This section discusses the research questions posed for this thesis in Chapter I.

1. Primary Research Question

What is the value of transitioning to IPv6?

The DoD will reap the rewards for starting the transition to IPv6 before the rest of the U.S. The architectural structure of the network is changing because of the new features in IPv6 and this makes the transition very complex.

Transitioning from IPv4 to IPv6 will prove to be a difficult challenge for the DoD and its networking personnel. The transition is going to happen, so the networking personnel are preparing for the change. It appears that the biggest challenge to IPv6 is that IPv4 networks administrators are satisfied with the inner workings of IPv4. After all, the IPv4 network provides the same capability as IPv6 through the use of extensions. The major difference is that IPv6 has the IPv4 extended capabilities built-in rather than added on, after the fact. With this information, there appears to be no rush by the American public to migrate to IPv6. The DoD could not afford to remain status quo with regard to IPv4. If the DoD had not mandated the transition, it may well have been at risk of being pushed into IPv6 in a relatively short timeframe.

Internet Protocol version 6 impacts the network addressing and routing mechanisms. All devices on the network will have a new address once the transition is completed. Proper planning has made IPv6 backward compatible with existing IPv4 installations. Tunneling or transition mechanisms will allow IPv4 and IPv6 to run at the same time on the same network.

The reports being filed by DoD organizations will provide the leadership the assurance that IPv6 is providing a strategic value. They will also provide the status of the transition so that progress can be made available for future decisions. The DoD made a good start by creating a transition office and centralizing the transition at DISA. The Services have also moved forward by creating their own transition offices.

The DREN pilot is a resource that will aid with the transition planning and implementation activities. This will result in a budgetary savings when compared to the consequence of ignoring the transition requirements. The transition has been sponsored by the DoD. The policy has been developed, but it does remain flexible so that adjustments to the schedule can be made. Since the transition has a high priority for the DoD, obtaining resources may be unproblematic when compared to traditional funding battles. The DoD has already made a valuable step to the transition by mandating that all equipment purchases be IPv6 capable. In addition to this mandate, the term "IPv6 capable" was defined by the DoD Transition Office to provide an end state to network administrators. The DoD must continue to expend resources on solving IPv6 problems and migrate away from solving IPv4 problems. Research and development is being conducted with VoIP, convergence, QoS, and other issues related to IPv6.

Internet Protocol version 4 will coexist with IPv6 for several years. There is every reason to believe that the transition can overlap with normal technology upgrades. It is just a matter of time before the DoD is IPv6 capable end-to-end. At that time, the DoD may take full advantage the new IPv6 features.

2. Subsidiary Research Question #1

How will the cost of the new protocol be assessed in terms of complexity and performance?

The research completed in this thesis suggests that the transition will continue to be complex and that the DoD will need to continue to push headlong into moving to IPv6. Beginning with an inventory of DoD equipment that is, or is not, IPv6 compatible is a good start to the overall process. The new protocol will not only need new equipment, but it will also require training and education for anyone involved with communication and Internet protocols. The DoD will need to expand it's testing and conformance beyond JITC down several subordinate layers of the DoD. The testing should start to expand to begin to understand the full requirement to transition to an IPv6 environment that will co-exist with IPv4.

3. Subsidiary Research Question #2

How will communication equipment be considered within the DoD?

The Department of Defense is currently seen as the leader in the United States for its advances toward transitioning to IPv6. Communication is always expensive and the refresh cycle associated with IPv6 compatible equipment is a means that will allow the DoD to catch up to the rest of the world with regard to transitioning to IPv6. There will be no support for IPv6 applications or services, only the transport mechanisms will be in place by 2008. The developers of IPv6 made IPv6 backward compatible with IPv4 via interoperability mechanisms. Since only the backbone is transitioning in 2008, there will only be support for the NIPRNet and Teleport. [17]

4. Subsidiary Research Question #3

Is it best to transition from the periphery or the core?

The Defense Information Systems Agency is implementing IPv6 over a DISN core Ipv4 backbone. The Ipv6 routing architecture / policy will remain the same as the DISN core Ipv4.

The potential security risks to Ipv6 will take time to uncover. Programmers that currently spend time attacking Ipv4 systems will undoubtedly begin to attack Ipv6 on a regular basis. When the core is Ipv6 capable, theoretically, attacks via covert channels should be held off by the periphery. However, hijacking the core and preventing data flow to/from the user community in the periphery can cause a denial of service. Another threat is the maintenance and refresh cycle. The system will continue to be vulnerable as long as a core or periphery device is still working off Ipv4. Services are provided at the

[17] Teleport: “The system will integrate, manage, and control a variety of communications interfaces between the Defense Information System Network (DISN) terrestrial and tactical satellite communications (SATCOM) assets at a single point of presence.” Retrieved on 27 Aug 2006 from http://www.disa.mil/main/prodsol/teleport.html

periphery, because the core primarily functions to forward traffic. The IPSec functionality is a periphery service and it is done at the first and last encountered Ipv6 device.

The current initiatives by the Navy indicate that transitioning from the core can be done as long as the necessary precautions are taken to avoid security risks. The problem is that there is no way to tell where security problems will arise until Ipv6 is more prevalent. Should the transition happen from the core to the periphery, the DoD will invite attackers to get directly into it's core network. If the transition begins from the periphery, this will allow the DoD to continue to test for security problems in Ipv6 without a significant threat to its core network. At the same time, research can be done to track the progress of attackers on the new protocol. As the attacks are identified, the DoD can protect itself against those known attacks and prevent them from getting to the core. As the risk of significant damage to the periphery is reduced, the core can then begin its transition to Ipv6.

This analysis indicates that there is no one correct answer with regard to transitioning from the core or the periphery. Both can be hazardous to the system. At the very least, the DoD should take an evolutionary approach to the transition. The transition should be made by starting with areas that will have the least impact on the system should it be attacked.

Transitioning from the core would undoubtedly have the highest risk of failure. This approach could result in a single point of failure where an attacker might only need to get past one router. Attack techniques can be tracked and mitigated at the periphery prior to the transition of the core. This would keep an attacker from getting past a router today that might have been thwarted by a security upgrade tomorrow. The system may be able to withstand an attack to a part of its periphery, but the same cannot be said for the core.

5. Subsidiary Research Question #4

What risks are involved with the transition?

Software, hardware, technology, cost, schedule, security, and people are all risks to the transition. Vendors in the United States will need to continue to develop software and hardware for IPv6. The DoD will also need to continue to purchase IPv6 compatible equipment so that companies will be motivated to not only produce quality products, but to also innovate and create new technologies to help support the warfighter. The United States needs to be concerned that it is falling behind the rest of the world in the transition to IPv6. It is possible that individual home users will not be affected by the transition since ISPs will eventually provide their customers with a dual-stack transition mechanism. The DoD plans to move beyond the dual-stack environment to a native IPv6 environment. Since the DoD has been directed to buy IPv6 capable equipment, it can be safely assumed that private ISPs will not be a reliable model for the DoD to follow with regard to transitioning the core. The ISPs can't control the transition of the private user, while the DoD can generate a directive that requires users to make the transition.

The scheduled transition is for June 2008; it is a certainty that the schedule will slip and prolong the DoD's risk associated with IPv4 traffic on the IPv6 network.

6. Subsidiary Research Question #5

Has the DoD declared its requirement for IPv6 products?

The DoD has not strictly declared it requirements, but it has inventoried its IPv6 compliant equipment. Once the technologies materialize, organizations will be able to enable IPv6 capable hardware. As long as interoperability is available and the market is big enough, users will likely adopt IPv6 hardware and software products.

7. Subsidiary Research Question #6

Have vendors invented new products or will the DoD first have to specify the requirement?

Internet Protocol version 6 products are being developed by U.S. and foreign countries. Vendors in the U.S. could reduce their costs by developing and deploying products that already have solutions for issues that were resolved in foreign countries.

The DoD should continue to realize the benefits of foreign IPv6 deployment as long as its IPv4 networks and applications can connect to IPv6 networks and applications.

8. Subsidiary Research Question #7

What is the DoD policy with regard to opening the core to new technology?

The DoD is working on a strategy that allows the core to be touched by IPv6 as long as all appropriate security measures have been taken. There are varying levels of IPv6 readiness in products. Most networking equipment is advertised as “IPv6-ready” or “IPv6-capable,” but network engineers must be aware of the differences between the basic functionality of one device and the advanced IPv6 functionality of another device.

The DoD is not currently working toward a native IPv6 environment, at any command, which would require all IPv4 to IPv6 transition mechanisms to be eliminated. The DoD will continue its transition to IPv6, but it will be saddled with both transition mechanisms and tunneling for the foreseeable future.

C. AREAS FOR FURTHER RESEARCH

The DoD will be looking to IPv6 to provide mobility to its force. This should be a driving factor behind IPv6 technologies in the DoD.

Continuing to run IPv4 may become impractical or more costly than transitioning to IPv6. The inventories submitted by agencies within the DoD can be reviewed and analyzed to determine whether or not organizations will want to transition to IPv6 or must be forced to do so as a result of a directive from higher headquarters.

A study of IPv6 in the U.S. can be conducted on both independent research and the collaboration of ideas with private stakeholders. The study should include the DoD’s communications networks and its ability to help U.S. companies compete in the global market for IPv6 products, networks, and services. It is important to disseminate information inside and outside of the DoD about the use of IPv6.

Testing of IPv6’s interoperability with existing IPv4 systems can be further researched as well as techniques to improve the performance and efficiency of IPv6 VoIP and mobile IPv6 routing. Continuous testing will need to be conducted for security in dual-stack environments, intrusion detection techniques for IPv6, performance in dual IPv4/IPv6 environments, Public Key Infrastructure scalability, and secure Border Gateway Protocol (BGP).

The transition for planning and execution is based on three Milestone Objectives found in the DoD Transition Plan. The DoD is currently in Milestone Objective 1 (MO1). Milestone Objective 2 (MO2) is scheduled to start on 1 October 2006. There will be "live" IPv6 packets on the GIG by the time MO2 begins; however, it will be confined to DoD networks and between pilot enclaves. The different milestones can be studied for their completeness and timeliness.

Only the DoD backbone is transitioning on 30 June 2008. The backbone transition consists of the NIPRNet and Teleport. There will be no support for IPv6 applications or services, only the transport mechanism. Future research of this subject can be done by revisiting the DISA IPv6 Implementation Plan. Additional information can also be obtained from the DoD IPv6 Transition Office.

Security can possibly be the subject for an entire research project. The NIST will publish a standards profile in November 2006 and technical guidance that focuses extensively on cybersecurity in early 2007.

D. CONCLUSIONS

If it weren’t for the DoD mandate to transition to IPv6 by 30 June 2008, it is likely that the United States would move to IPv6 much later than Europe and Asia. This is apparent because service providers are currently using the IPv6 network in countries other than the U.S. Many publications indicate that administrators in the U.S. believe the extensions provided by IPv4 are just as good as the built-in features of IPv6. The DoD is creating a market for IPv6 equipment and software in the U.S., as the mandate included a requirement for the acquisition of all new computer equipment to be IPv6 capable. As a result, companies such as CISCO have been selling IPv6 compatible equipment for a couple of years. The DoD’s market share of the U.S. component of the Internet is not as influential over the status of the Internet as was DoD’s influence over the development and advancement of the networks that ultimately culminated in the Internet. Thus, the DoD must continue to aggressively coordinate and support the development of IPv6 standards, protocols, and conformance if it holds the transition to be one of its core interests. It must be an active participant in identifying and facilitating solutions for technological and interoperability issues. It is in the best interest of the DoD that it continue to be a major factor in stimulating the adoption of IPv6 by being a major consumer of IPv6 products and services.

Various publications and interviews were used to compile the qualitative data collected and analyzed in this thesis. The consensus of various experts overwhelmingly indicated that the U.S. as a whole needs to transition to IPv6 in order to maintain its place at the forefront of technology innovation. There is some debate, however, as to the most beneficial timeline. Some believe that the DoD's push is necessary to lead the charge to IPv6, others believe that IPv6 will make the transition through a more natural progression. The global view of IPv6 indicates that if the U.S. does not transition with the rest of the world, it could be left with transition mechanisms and security holes, leaving the world to look inside its network. The idea that the extended security features of IPv4 are just as good as the built-in security of IPv6 may be valid, but the DoD should continue it's move to IPv6.

An advisory of security issues concerning IPv6 was issued by the Department of Homeland Security, according to OMB memorandum 05-22. It appears that the DoD wants to avoid possible security issues, since it will be a part of the IPv6 network, be it by tunneling or using transition mechanisms. In June 2008, all agencies' network backbones must be using IPv6 and agency networks must interface with this infrastructure. Guidance was published to ensure an orderly and secure transition from IPv4 to IPv6, because the Internet Protocol is core to the agency's IT infrastructure.

The Federal transition to IPv6 is progressing slowly, but the momentum may be picking up. Most agencies have submitted their final official transitional reports to OMB, but the networks must still be upgraded. Guidance is being prepared for agencies to migrate their network backbones to the new Internet Protocol.

The commands should be able to meet the IPv6 requirement through routine upgrades and technology refreshes. Additional resources may be needed for ongoing planning, training, labor, the management of the transition and the resulting dual-stack network implementation. Many agencies do not understand how they will be using the new protocol; therefore, asking for and receiving funding may prove to be difficult.

The DoD has an IPv6 certification program to help test for compliance, but the move to a fully functional, native IPv6 network will not be available by June 2008. Project planners are testing these new technologies that will be used in the next 10 years.

An important DoD resource for research and engineering is the DREN. The DREN provides a strong interconnectivity with other major networks and high performance test beds. It is a resource that enables wider user of IPv6 by the DoD research community and should be leveraged accordingly.

E. RECOMMENDATIONS

1. The DoD Should Continue Its Transition to IPv6 Without a Deadline as Close as June 2008

As industry develops IPv6 compatible equipment, it will undoubtedly get better and more efficient and cost effective. Time will also allow those who attack computer systems to reveal their treachery. In the meantime, the DoD will be able to adjust its timeline for the acquisition of equipment as well as policies regarding its computer infrastructure. Delaying the acquisition of equipment will allow the DoD to take advantage of more secure equipment and software as they become available. The time will also allow for more in-depth testing for conformance. Testing and acquisition should continue, however, the transition deadline could easily be pushed back a couple, if not a few, years.

2. The DoD Should Expand Its Test Bed

Currently, the test beds are limited to a few specific sites in the DoD. This testing should be shared with several commands, to include the necessary equipment to conduct long distance analysis. This will require that the DoD invest in specialists that work in the IP field. These specialists will need to be at each test site and will need to be employed for the next three to five years.

3. The DoD Should Develop Formal IPv6 Training and Education.

The specialized skills taught to military members in the computer science specialty will need to include knowledge about IPv6. This training would need to be inserted into the curriculum while the students are in the accession pipeline. This training will also need to be presented in the advanced courses. They will need to be experienced with both IPv4 and IPv6 so that they will be conversant in both protocols. If they are not formally trained in the schoolhouse, they will have to learn about IPv6 on the job. This may not be the best place to learn about IPv6, since it is the inexperienced that often get taken advantage of by more experienced attackers.

4. The DoD Should Increase Its Participation in Local, Regional, National, and International Meetings Designed to Develop the Next Generation Protocol.

This thesis found that, relatively speaking, there are only a handful of DoD personnel participating in conferences related to IPv6. There have been DoD sponsored conferences, but military participation should be increased beyond its current level.

5. The DoD Should Expand Its Testing Influence and Participation.

The DoD could expand its support of standards and interoperability testing being developed and performed by the University of New Hampshire and the European Telecommunications Standards Institute (ETSI). The testing has been assigned to one agency, but that testing could be expanded to include other agencies and subordinate commands. The testing should remain centralized under DISA to ensure that DoD IPv6 fielding is coordinated, does not duplicate efforts, and does not introduce interoperability or assurance risks. There should be testing by other organizations under the lead of DISA and it should be more aggressive.

6. Additional Human Resources Must Be Dedicated to the Standards.

The research effort can only be sustained if the DoD builds a base of skilled human resources. The specific research focus areas should include interoperability, security, and transition mechanisms. The DoD should support the development of new applications and initiate test beds in addition to Moonv6.

F. POTENTIAL FUTURE RESEARCH QUESTIONS

For networks that have not transitioned to IPv6, how has the maintenance of the IPv4 network affected security? How has it affected the budget? How has it affected the acquisition of IPv4 capable equipment?

Has the DoD's push to make the transition to IPv6 helped or hindered the market? Have shortcuts been taken to in order to meet the equipment and services demands of the DoD? How involved is the DoD with getting IPv6 information to its users, administrators, and school houses?

How has IPv6 affected mobile communications? Is there an architecture in place that allows IPv6 to be used by the operating forces on the move? Does IPv6 equipment pass conformance tests?

Are the Milestone Objectives on schedule? If not, what can be done to get them back on track? Do the live packets on the GIG meet the intended criteria? What security risks surfaced after the live packets hit the GIG?

What is the status of IPv6 applications and service support? What guidance has been released since the transition plan of 2005?

What equipment has been conformance tested for security? What percentage of the tested equipment meets the security criteria set by NSA? Has NSA approved encryption devices that satisfy the intelligence community at large?

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A: AGENCY IPV6 INVENTORY GUIDANCE

This appendix contains the format used to collect an inventory on existing devices. The agencies were directed to conduct an inventory of existing IP-aware switches, routers, and hardware firewalls. The inventory was to be conducted per "investment" as defined in OMB Circular A-11, section 53. The first inventory had to be reported to OMB no later than November 15, 2005.

Agencies also had to provide a second inventory of all IP compliant devices and technologies not captured by the first inventory. Agencies were directed to provide a progress report as part of their February 2006 Enterprise Architecture (EA) submission to OMB. This inventory must be completed and reported to OMB no later than June 30, 2006.

Both inventories were to include the data elements found in Table 1, below, for each device/technology:

IPv6 Transition Checklist			
1. Investment (Name)			
Investment Name:	InvestmentBY06 UPI:		
Agency:	Sub-Agency:		
Program Manager:	Phone: Email:		
Prime Support Contractor:			
2. Investment Information			
a. Investment Description:			
Number of Distinct Types of Applications/Devices:	Percent of Applications/Devices IPv6 Compliant:		Number of Distributed Sites Associated with this Investment
3. Identify Applications or Devices used within this investment: (Add more lines as required, see Type Code legend below) - Additional details are required for complete inventory at the bottom of this report.			
Application/Device Name (Acronym)	Purpose	Type	Manufacturer/Vendor Name

Type Code Legend: **G** = Government Off-the-Shelf **C** = Commercial Off-the-Shelf **MC** = COTS Modified by Government Contract but still **S** = Shareware **F** = Freeware available to the public **RT** = Router Device **FD** = Firewall Device **SW** = Switch Device **AD** = Authentication Device **OD** = Other Device **VD** = VPN/Remote Access Device available to the public. **HD** = Host Device **CD** = Client Device .			
4. Identify Applications or Devices that are not IPv6 compliant			
Application/Device Name (Acronym)	Describe dependence on IPv4	Impact (see Legend)	IPv6 Compliant Date
Impact Code Legend: **Legacy** = App/Device will be replaced before 2008 and will not transition. **Mod** = Will be modified by date identified **Upgrade** = New IPv6 compliant version will be implemented by date identified **Waiver** = Waiver will be submitted per guidance in Transition Plan			
5. Identify reliance on IPv4:			
a. Define how IPv4 is implemented preventing IPv6 capability: (Database fields; hard-coded addressing; proprietary protocol implementation; IPv4 loopback addresses; reliance on non-IPv6 OS, COTS, or GOTS)			
b. Identify the amount of IPv4 address space used by the investment in terms of approximate CIDR address blocks, e.g. /20, /24, etc.			
6. Technical impact of transition to IPv6:			
a. Describe what needs to be done to achieve initial dual stack capability and/or full transition to IPv6.			
b. Describe IPv6 characteristics that will or should be leveraged as part of the system's architecture (i.e. stacked headers, site/link local addressing, mobile IPv6, IPSec, unicast/multicast/anycast, stateless autoconfiguration).			
7. Dependencies:			
a. Describe technical dependencies that will impact the IPv6 implementation, i.e. processor or memory constraints, APIs, etc.			
b. Describe logistical dependencies external to your system, i.e. interrelated programs (C2PC, TDN, etc.) Upper Layer Protocols and applications.			
8. Programmatic impact(s):			
a. Schedule for systems to be dual-stack and full IPv6 compliant using current Development Schedule. Include deployment, fielding, upgrade, and retrofit milestones.			
(1) Cost schedule – list currently budgeted, such as for tech refresh or upgrade, and additional funding required (deficiency) for each FY to achieve initial and objective IPv6 capabilities in 8a. EXAMPLE: FY07 $20K($5K), FY08 $8K($0)			
b. Accelerated schedule for systems to be dual-stack and full IPv6 compliant if current Development Schedule does not meet the goal of IPv6 compliant by 2008. Include deployment, fielding, upgrade, and retrofit milestones.			
(1) Cost schedule – list currently budgeted, such as for tech refresh or upgrade, and additional funding required (deficiency) for each FY to achieve initial and objective IPv6 capabilities in 8b. EXAMPLE: FY07 $20K($5K), FY08 $8K($0)			
9. Define technical and programmatic risks.			
10. Define Risk Mitigation Strategy for items identified in block 9.			
11. Can this investment or the systems in the investment become a representative "early adopter"? (Yes / No)			
12. Recommendations: (Enter any comments or ideas you have that have a bearing on this initiative)			

Application and Device Inventory

(Additional details continued from question #3 above)

Application/Device Name (Acronym)	Version /OS	Device ID/ Serial number	Cost (000s)	Device Capabilities (IPv4,IPv6, dual stack)	For Firewall Devices: Does Device have the ability to monitor tunneled IPv6 traffic (Type 41 Packets) and conduct Deep Packet Inspection (Yes / No)	Supported Standards	Manufacturer Upgrade Plan	Technical Refresh Date	Device Security Level/Criticality	Known Issues with Device

Table 2. Agency IPv6 Inventory Guidance (From: OMB, 2005)

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B: IMPACT ANALYSIS

This appendix contains a description of the impact analysis that was to be completed by November 15, 2005. The agencies were to provide progress as part of the February 2006 agency EA submission to OMB. The results of this impact analysis are to be reported to OMB no later than June 30, 2006 and must include both cost and risk elements as described in OMB Circular A-11.

Cost estimate should include:

1. Planning
2. Infrastructure Acquisition (above and beyond normal expenditures)
3. Training
4. Risk mitigation cost

Risk Analysis should consider:

1. Schedule
2. Technical obsolescence
3. Feasibility
4. Reliability of systems
5. Dependencies and interoperability issues
6. Surety (asset protection) considerations
7. Risk of creating a monopoly for future procurements
8. Capability of agency to manage the investment
9. Overall risk of investment failure
10. Organizational and change management
11. Business
12. Data/info
13. Technology
14. Strategic
15. Security
16. Privacy
17. Project resources
18. Human capital

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C: TRANSITION ACTIVITIES NOTIONAL SUMMARY

This appendix contains guidance for the CIO Council so that it could develop additional transition guidance. The agencies were directed to address the actions as soon as possible. Beginning February 2006, agencies' transition activity was to be evaluated using OMB's Enterprise Architecture Assessment Framework:

1. Conduct a requirements analysis to identify current scope of IPv6 within an agency, current challenges using IPv4, and target requirements.
2. Develop a sequencing plan for IPv6 implementation, integrated with your agency Enterprise Architecture.
3. Develop IPv6-related policies and enforcement mechanisms.
4. Develop training material for stakeholders.
5. Develop and implement a test plan for IPv6 compatibility/interoperability.
6. Deploy IPv6 using a phased approach.
7. Maintain and monitor networks.
8. Update IPv6 requirements and target architecture on an ongoing basis.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

1. Agilent Technologies, Inc. (April 2004). *Ipv6 Transition Test Challenges*. White Paper.

2. Alberts, D., Garstka, J., and Stein, F. (February 2000). *Network Centric Warfare: Developing and Leveraging Information Superiority*. Second edition (Revised). DoD C4ISR Cooperative Research Program, (CCRP publication series).

3. Article. (9 Jan 06). *Realizing the Benefits of IPv6 Will Take Time*. Retrieved on 27 April 2006 from http://www.gcn.com/print/25_01/37897-1.html

4. AT&T Labs Research Team (2005). White paper. *New Generation of the Internet Protocol*.

5. Baird, J. (October 2004). DREN IPv6 Pilot Network brief prepared by the DoD High Performance Computing Modernization Program (HPCMP) Office, released for distribution by SPAWAR Systems Center, San Diego, Special Document SD570.

6. Bernstein, D. J., (nd), *The IPv6 Mess*. Internet publication, retrieved on 10 January 2006 from <http://cr.yp.to/djbdns/ipv6mess.html>.

7. Buxbaum, P. (13 March 2006). *Network Transition*. Military Information Technology, Volume 10, Issue 2. Retrieve on 5 August 2006 from http://www.military-information-technology.com/article.cfm?DocID=1348

8. Carpenter, B. and Jung, C. *Transmission of IPv6 over IPv4 Domains without Explicit Tunnels*, RFC 2529. March 1999.

9. Carpenter, B. and Moore, K. *Connection of IPv6 Domains via IPv4 Clouds*, RFC 3056. February 2001.

10. Charny, B. (23 July 2003). *U.S. Shrugs off World's Address Shortage*, CNET News.com, Published on ZDNet News. Retrieved 30 January 2006 from <http://news.zdnet.com/2100-3513_22-5055803.html>.

11. Chauhan, Y. (Not dated). *Security in the Wake of IPv6*. Indian Institute of Technology Kanpur.

12. Chen, W., Lin, Ying-Dar, and Lin Yi-Neng. (2004). *Tunnel Minimization and Relay for Managing Virtual Private Networks*. Department of Computer and Information Science National Chiao Tung University Hsinchu, Taiwan. IEEE Communication Society. Globecom.

13. Choi, D. (1 May 2006). Defense Information System Agency brief by Don Choi entitled DISN IPv6 Implementation Plan at the DISA Customer Partnership Conference.

14. CIO Council Architecture and Infrastructure Committee (AIC), *Integrating IPv6 into Agency Enterprise Architecture Planning*, Office of Management and Budget (OMB), November 15, 2005.

15. Comer, D., *Computers and Internet Networks with Internet Applications*, 4th Edition, pp. 280-281, Pearson Education, Inc., 2004.

16. Crawford, M. & Huitema, C. *DNS Extensions to Support IPv6 Address Aggregation and Renumbering*, RFC 2874. July 2000.

17. Davies, J. (2003). *Understanding IPv6*. Microsoft Press.

18. Dixon, R. (not dated). *IPv6 in the Department of Defense*. Joint Interoperability Test Command brief for the Defense Information Systems Agency.

19. Duncan, Richard Jeremy (7 August 2006). Information provided by Captain Jeremy Duncan, USMC, via E-mail from his post as C4I Interoperability Officer at the Joint Interoperability Test Command, Fort Huachuca, AZ.

20. Durand, A., Fasano, P., Guardini, I. and Lento, D. *Tunnel Broker*, RFC 3053. January 2001.

21. Evans, M. (2005). *Navy IPv6 Transition*. Navy IPv6 Transition Project Office COMSPAWARSYSCOM, Office of the Chief Engineer. Retrieved in 4 August 2006 from http://www.usipv6.com/6sense/2005/dec/01.htm

22. Fujisawa, K. and Onoe, A. *Transmission of IPv6 Packets over IEEE 1394 Networks*. October 2001

23. Gallaher, M. (February 2006). *Converting to New Internet Protocol Will Cost $25 Billion*. RTI International News Release. Retrieved 20 May 2006 from http://www.rti.org/newsroom/news.cfm?nav=364&objectid=9B3F489C-28CF-49F8-85034CF7FE6B708D

24. Geesey, D. (nd), IPv6 Transition Workshop. Retrieved 26 March 2006 from http://www.v6training.com/.

25. Gilligan, R. & Nordmark, E. *Transition Mechanisms for IPv6 Hosts and Routers*, RFC 2893. August 2000.

26. Gritter, Geoffrey. (Mar 00). *IPv6 Deployment Challenges and Risks*. http://www-dsg.stanford.edu/papers/triad/node24.html

27. Guardini, I., (nd), *Migrating from IPv4 to IPv6: Planning an Effective IPv6 Transition*. Retrieved 13 January 2006 from <http://carmen.cselt.it/papers/globalIPsummit-v6trans/ipv6-transition-summary.html>.

28. Guzelian, M., and Limoges, C. (February 2006). 6Sense Article. *The Challenges of Transition – T*he Move from ATM and IPv4 to IPv6. IPv6 Summit, Inc. Retrieved on 27 August 2006 from http://www.usipv6.com/6sense/2006/feb/03.htm

29. Hagino, J. and Yamamoto, K. *An IPv6-to-IPv4 Transport Relay Translator*, RFC 3142. June 2001.

30. Harrison, Ric, Schlabach, Jerry, Millane, Dan, Smith, Shawn. (Nov 2005). *JITC Supports Advanced Joint Internet Protocol Interoperability Testing and Transformation Initiatives.* Article.

31. Hauben, R. (23 June 1998). *From the ARPANET to the Internet. Columbia University*. Retrieved on 27 August 2006 from http://www.columbia.edu/~rh120/other/tcpdigest_paper.txt

32. Hawk, J. (August 2005). *Wireless Warriors Secure in Their Knowledge*. SIGNAL, AFCEA's International Journal. Retrieved on 27 August 2006 from http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=1000&zoneid=163

33. InterOperability Laboratory, UNH-IOL IPv4 Consortium, retrieved 27 March 2006 from <http://www.iol.unh.edu/consortiums/ipv4/>.

34. IPv6 Transition Technologies, (12 September, 2005). Retrieved on 9 January 2006 from <http://www.microsoft.com/windowsserver2003/techinfo/overview/ipv6coexist.mspx>.

35. IPv6. IPv6 Task Force, U.S. Department of Commerce, (January 2006). *Technical and Economic Assessment of Internet Protocol Version 6 (IPv6).* Retrieved on 14 May 06 from <http://www.ntia.doc.gov/ntiahome/ntiageneral/ipv6/final/IPv6final.pdf>.

36. Jackson, W. (14 August 06). *IPv6: The future is now*. GCN Staff. http://www.gcn.com/print/25_24/41632-1.html

37. Jackson, W. (3 April 06). *Don't look for rapid ROI from IPv6*. GCN Staff. http://www.gcn.com/print/25_7/40237-1.html?topic=IPv6

38. Jackson, W. (9 Jan 06). *Will IPv6 networks be ready to handle Government's needs?* GCN Staff. http://www.gcn.com/print/25_01/37899-1.html

39. Kreidler, T., (2006). *Mastering the IPv6 Transition*. Juniper Networks. Retrieved on 30 August 2006 from http://www.usipv6.com/6sense/2006/may/article06.htm

40. Lost. (3 April 2006). *Lost in Transition*. GCN Tech Report, not author identified. Retrieved on 14 July 2006 from http://www.gcn.com/print/25_7/40236-1.html

41. Lovering, N. (27 April 2006). *The Impact of IPv6 on Semantic Interoperability*. Cisco Systems brief.

42. Miller, J. (3 Apr 06). *Agencies find there's no single path to IPv6*. GCN Staff. http://www.gcn.com/print/25_7/40248-1.html?topic=IPv6

43. Mitchell, B. (ND). *Internet Protocol Tutorial*, retrieved 3 May 2006 from <http://compnetworking.about.com/od/tcpiptutorials/a/ipaddrnotation.htm>.

44. Murphy, Robert, (2006). A conversation with Captain Robert Murphy, USMC at the Naval Post Graduate School, Monterey, CA.

45. Nordmark, E., S*tateless IP/ICMP Translation Algorithm (SIIT)*, RFC 2765. February 2000.

46. Internet Glossary of Terms. Retrieved on 21 May 2006 from http://www.ez-access.com/glossary.html

47. O'Neal, M. R., June 2003, *A Design Comparison Between IPV4 and IPV6 in the Context of MYSEA, and Implementation of an IPv6 MYSEA Prototype*. NPS Thesis.

48. Office of ASD(NII)/DoD CIO, *The Department of Defense (DoD) Internet Protocol Version 6 (IPv6) Transition Plan*, Version 1, Unclassified\\For Official Use Only, Department of Defense (DoD), March 2005.

49. OMB. Office of Management and Budget (OMB) memorandum, SUBJECT: *Transition Planning for Internet Protocol Version 6 (IPv6)*. August 2, 2005.

50. Osmundson, J., (April 2006). Research Associate Professor of Information Sciences (1995) Ph.D., University of Maryland, 1968. Information was gathered during a Software Project Management class at the Naval Postgraduate School, Monterey, CA.

51. Palet, J. (undated) Brief entitled *IPv6 Commercial Deployment in Europe*. European IPv6 Task Force & Steering Committee IPv6 Forum.

52. Partridge, C. & Jackson, A. *Stateless IPv6 Router Alert Option*, RFC 2765. October, 1999.

53. Patterson, T. (May 2006). *Show Time*. FedTech Magazine. Retrieved on 4 June 2006 from http://www.fedtechmagazine.com/article.asp?item_id=202

54. Pervasive Technology Labs, Indiana University. (31 March 2003). *Advanced Networking Management Lab (ANML) Internet Protocol, Version 6 (IPv6) Resources*. Retrieved on 3 June 2006 from http://www.anml.iu.edu/ipv6/resources/whyipv6.html

55. Pollock, S. (March 2004). *IP Version 6 NCAR*. Federal West Consulting Team. Retrieved on 4 August 2006 from http://www.cisl.ucar.edu/nets/docs/ipv6/pollock_ipv6_ncar.pdf

56. Postel, J., *Internet Protocol*, RFC 791. September 1981.

57. *Pv6 Features*. (21 January 2005). Retrieved on 3 June 2006 from http://technet2.microsoft.com/WindowsServer/en/Library/7dc20b9e-6538-429d-b222-81eb6b7fcdfb1033.mspx?mfr=true

58. SecNet 54™. (2006). SecNetTM Data Sheet Type 1 Secure Internet Protocol Encryptor. Retrieved on 27 August 2006 from http://download.harris.com/app/public_download.asp?fid=1015

59. Sorby, K. (July 2003) *Relationship Between Security and Safety in a Security-Safety Critical System: Safety Consequences of Security Threats*. HoveDoppgave. Retrieved 4 June 2006 from http://www.idi.ntnu.no/grupper/su/su-diploma-2003/sorbySafetySecurity.pdf

60. Spaulding, J. (April, 2005). *AF IPv6 Transition Challenges*. Air Force IPv6 Transition Management Office (TMO), AFCA/ECSS. Retrieved on 4 August 2006 from http://www.opengroup.org/gesforum/doc.tpl?CALLER=documents.tpl&dcat=&gdid=7426

61. Spirent Communications, Inc. (July 2004). *IPv6 and the Next Generation Internet Protocol Overview*. White Paper

62. Tech Watch Report, (2006). Internet Article, *Migrating Everything to 'IP'*. Retrieved on 20 May 2006 from http://www.fcw.com/vendorsolutions/techwatch/migrate.asp.

63. TechNet, (21 January 2005). *IPv6 Address Space*, retrieved 3 May 2006 from < http://technet2.microsoft.com/WindowsServer/en/Library/9b665bd3-84a8-4ca0-8f20-bc5fb58b6dc81033.mspx>.

64. Volpe, C. (1 Aug 2006). *Latest UNH-IOL 'Moonv6' Test Launches IPv6 Application Testing*; Industry Group Test Includes First Public Demo of Network Time Protocol over Native IPv6. Retrieved on 4 August 2006 from http://home.businesswire.com/portal/site/google/index.jsp?ndmViewId=news_view&newsId=20060801005998&newsLang=en

65. Warfield, M. (2003). *Security Implications of IPv6*. Internet Security Systems.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Fort Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Marine Corps Representative
   Naval Postgraduate School
   Monterey, California

4. Director, Training and Education, MCCDC, Code C46
   Quantico, Virginia

5. Director, Marine Corps Research Center, MCCDC, Code C40RC
   Quantico, Virginia

6. Marine Corps Tactical Systems Support Activity (Attn: Operations Officer)
   Camp Pendleton, California

7. Associate Professor Geoffrey Xie (Computer Science)
   Naval Postgraduate School
   Monterey, California

8. Research Associate John H. Gibson (Computer Science)
   Naval Postgraduate School
   Monterey, California

9. Professor Dan C. Boger
   Naval Postgraduate School
   Monterey, California

10. Major Peter Hart, United States Marine Corps
    Marina, California